

# SUPER-APPROXIMATION, I: $\mathfrak{p}$ -ADIC SEMISIMPLE CASE.

ALIREZA SALEHI GOLSEFIDY

ABSTRACT. Let  $k$  be a number field,  $\Omega$  be a finite symmetric subset of  $\mathrm{GL}_{n_0}(k)$ , and  $\Gamma = \langle \Omega \rangle$ . Let

$$\mathcal{C}(\Gamma) := \{\mathfrak{p} \in V_f(k) \mid \Gamma \text{ is a bounded subgroup of } \mathrm{GL}_{n_0}(k_{\mathfrak{p}})\},$$

and  $\Gamma_{\mathfrak{p}}$  be the closure of  $\Gamma$  in  $\mathrm{GL}_{n_0}(k_{\mathfrak{p}})$ . Assuming that the Zariski-closure of  $\Gamma$  is semisimple, we prove that the family of left translation actions  $\{\Gamma \curvearrowright \Gamma_{\mathfrak{p}}\}_{\mathfrak{p} \in \mathcal{C}(\Gamma)}$  has *uniform spectral gap*.

As a corollary we get that the left translation action  $\Gamma \curvearrowright G$  has *local spectral gap* if  $\Gamma$  is a countable dense subgroup of a semisimple  $p$ -adic analytic group  $G$  and  $\mathrm{Ad}(\Gamma)$  consists of matrices with algebraic entries in some  $\mathbb{Q}_p$ -basis of  $\mathrm{Lie}(G)$ . This can be viewed as a (stronger)  $p$ -adic version of [BISG, Theorem A], which enables us to give applications to the Banach-Ruziewicz problem and orbit equivalence rigidity.

## CONTENTS

1. Introduction	2
1.1. Statement of the main result.	2
1.2. Applications.	3
1.3. Comparing with the previous related works.	5
Acknowledgments.	5
2. Preliminary results	5
2.1. Spreading of weight under convolution, and $l^2$ -flattening.	5
2.2. Regularization.	6
2.3. Reduction to the connected, simply-connected case.	7
2.4. Strong approximation and the $\mathfrak{p}$ -adic closures of $\Gamma$ .	9
2.5. Ping-pong players and the main result of [SGV12].	11
2.6. Summary of the initial reductions.	12
2.7. Escaping from subschemes, and ramified primes of a scheme.	12
2.8. Multiplicity bound.	15
2.9. Finite logarithmic maps.	16
3. Expansion, approximate subgroup, and bounded generation.	18
3.1. Statements and notation.	18

---

*Date:* February 2, 2016.

1991 *Mathematics Subject Classification.* 22E40.

A. S-G. was partially supported by the NSF grants DMS-1160472, DMS-1303121 and A. P. Sloan Research Fellowship. Parts of this work was done when I was visiting Isaac Newton Institute and the MSRI, and I would like to thank both of these institutes for their hospitality.

3.2. Theorem 30 (Approximate subgroup) implies Theorem 1 (Spectral gap).	18
3.3. Theorem 31 (Bounded generation) implies Theorem 30 (Approximate subgroup).	20
3.4. Proposition 32 (Thick top slice) implies Theorem 31 (Bounded generation).	20
4. Proof of Proposition 32 (Thick top slice).	23
4.1. Finding a basis consisting of vectors with small height.	23
4.2. Large number of conjugacy classes.	25
4.3. Helfgott's trick to get large centralizer.	27
4.4. Measuring the regularity.	28
4.5. Hitting shifts of regular semisimple elements.	30
4.6. Finding a torus with lots of $p$ -adically large elements in $A.A$ .	32
4.7. Proof of Proposition 32	34
5. Appendix A: a small solution.	38
5.1. Logarithmic height, and the statement of the main result.	38
5.2. Reduction to the geometrically zero-dimensional case.	39
5.3. Reduction to the complete intersection, geometrically zero-dimensional case.	40
References	41

## 1. INTRODUCTION

**1.1. Statement of the main result.** For a symmetric probability measure<sup>1</sup>  $\mu$  with finite support on a compact group  $G$ , let

$$T_\mu : L^2(G) \rightarrow L^2(G), \quad T_\mu(f) := \mu * f,$$

where  $(\mu * f)(g) := \sum_{g' \in \text{supp } \mu} \mu(g') f(g'^{-1}g)$ . It is easy to see that  $T_\mu$  is a self-adjoint operator,  $\|T_\mu\| = 1$ , and  $T_\mu(\mathbb{1}_G) = \mathbb{1}_G$  where  $\mathbb{1}_G$  is the constant function one on  $G$ . Let  $L^2(G)^\circ := \{f \in L^2(G) \mid f \perp \mathbb{1}_G\}$ . Hence  $T_\mu$  induces a self-adjoint operator  $(T_\mu)|_{L^2(G)^\circ}$  on  $L^2(G)^\circ$ , and let  $\lambda(\mu; G) := \|(T_\mu)|_{L^2(G)^\circ}\|$  be its operator norm. Notice that, if eigenvalue 1 has multiplicity one, then

$$\lambda(\mu; G) = \sup\{|\lambda| \mid \lambda \in \text{spec}(T_\mu), \lambda < 1\}.$$

We say  $\mu$  has *spectral gap* if  $\lambda(\mu; G) < 1$ . So if the group generated by the support of  $\mu$  is dense in  $G$ , the random-walk on  $G$  with respect to  $\mu$  equidistributes exponentially fast if  $\mu$  has spectral gap. The following *uniform spectral gap* is the main result of this article.

**Theorem 1.** *Let  $\Omega$  be a finite symmetric subset of  $\text{GL}_n(k)$ , where  $k$  is a number field. Let  $\Gamma = \langle \Omega \rangle$  and  $\Gamma_{\mathfrak{p}}$  be its closure in  $\text{GL}_n(k_{\mathfrak{p}})$  for any finite place  $\mathfrak{p}$  of  $k$ . Let  $\mathcal{C} := \{\mathfrak{p} \in V_f(k) \mid \Gamma_{\mathfrak{p}} \text{ is compact}\}$ .*

*Suppose the Zariski-closure  $\mathbb{G}$  is a semisimple group. Then there is  $\lambda_0 < 1$  such that*

$$\sup_{\mathfrak{p} \in \mathcal{C}} \lambda(\mathcal{P}_\Omega; \Gamma_{\mathfrak{p}}) \leq \lambda_0 < 1,$$

*where  $\mathcal{P}_\Omega$  is the probability counting measure on  $\Omega$ .*

---

<sup>1</sup>A measure  $\mu$  is called symmetric if  $i^*(\mu) = \mu$  where  $i : G \rightarrow G, i(g) := g^{-1}$ .

It is standard (see Lemma 12) that we can pass to a finite-index subgroup. So we can assume that, for some  $g \in GL_n(k)$ ,

$$g\Gamma g^{-1} \subseteq GL_n(\mathcal{O}_{\mathfrak{p}})$$

for any  $\mathfrak{p} \in \mathcal{C}$  where  $\mathcal{O}_{\mathfrak{p}}$  is the ring of integers of  $k_{\mathfrak{p}}$ . So we can and will assume that  $\Gamma_{\mathfrak{p}} \subseteq GL_n(\mathcal{O}_{\mathfrak{p}})$ . In particular, we can restrict the residue map  $\pi_{\mathfrak{p}^m} : GL_n(\mathcal{O}_{\mathfrak{p}}) \rightarrow GL_n(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^m)$  to  $\Gamma_{\mathfrak{p}}$ . It is well-known that Theorem 1 is equivalent to saying that the family of Cayley graphs

$$\{\text{Cay}(\pi_{\mathfrak{p}^m}(\Gamma), \pi_{\mathfrak{p}^m}(\Omega)) \mid \mathfrak{p} \in \mathcal{C}, m \in \mathbb{Z}^+\}$$

is a family of expanders if  $\Gamma$  and  $\mathcal{C}$  are as above and the Zariski-closure  $\mathbb{G}$  of  $\Gamma$  is semisimple. Such graphs are extremely useful in communication and theoretical computer science (see a survey by Hoory, Linial and Wigderson [HLW06]). In the past decade they have been found to be extremely useful in a wide range of pure math problems, e.g. affine sieve [BGS10, SGS13], sieve in groups [LM13], variation of Galois representations [EHK12], etc. (see [BO14] for a collection of surveys of related works and applications).

**1.2. Applications.** The application of Theorem 1 to new robust construction of family of expander graphs has been mentioned. Here are a few other applications.

**1.2.1. Local spectral gap.** In a recent work Boutonnet, Ioana, and the author [BISG] introduced *local spectral gap* for a measure class preserving action, and proved many interesting properties of such actions. As an application of Theorem 1, we get local spectral gap in the  $p$ -adic setting:

**Theorem 2.** *Let  $G$  be a semisimple  $p$ -adic analytic group. Let  $\Gamma$  be a countable dense subgroup of  $G$ . Suppose that  $\text{Ad}(\Gamma)$  consists of elements with algebraic entries in some  $\mathbb{Q}_p$ -basis of  $\text{Lie}(G)$ .*

*Then the left translation action  $\Gamma \curvearrowright (G, m_G)$  has local spectral gap.*

*Proof.* By [BISG, Remark 1.5], we are free to choose any measurable subset  $B \subseteq G$  with compact closure and non-empty interior and prove that the left translation action  $\Gamma \curvearrowright (G, m_G)$  has local spectral gap with respect to  $B$ . So, since  $G$  is  $p$ -adic analytic, we can and will assume that  $B$  is a (topologically) finitely generated pro- $p$  group. Hence the Frattini subgroup  $\Phi(B)$  is an open subgroup of  $B$ . Since  $\Gamma$  is dense in  $G$ , for any coset  $b\Phi(B)$  of  $\Phi(B)$  in  $B$  there is  $\gamma_b \in \Gamma \cap b\Phi(B)$ . Hence there is a finite symmetric subset  $\Omega$  of  $\Gamma \cap B$  which maps onto  $B/\Phi(B)$ . Thus  $\langle \Omega \rangle$  is a dense subgroup of  $B$ .

By our assumption, there is a number field  $k$  and a  $\mathbb{Q}_p$ -basis  $\mathfrak{B}$  of  $\text{Lie}(G)$  such that all the entries of  $\text{Ad}(\Omega)$  in the basis  $\mathfrak{B}$  are in  $k$ . Note that  $k$  comes with an embedding into  $\mathbb{Q}_p$ . Let  $\mathfrak{p}_0$  be the corresponding place of  $k$ . Let

$$\Gamma_0 := \langle [\text{Ad}(\Omega)]_{\mathfrak{B}} \rangle \subseteq GL_{\dim G}(k),$$

and  $\mathbb{G}_0$  be its Zariski-closure in  $(GL_{\dim G})_k$ . Since  $\Gamma_0$  is dense in an open subgroup of  $G$ , we have that  $G$  and  $\mathbb{G}_0(k_{\mathfrak{p}_0}) = \mathbb{G}_0(\mathbb{Q}_p)$  are locally isomorphic. Therefore  $\mathbb{G}_0$  is semisimple. So by Theorem 1 we have  $\lambda(\mathcal{P}_{\Omega}; \text{Ad}(B)) < 1$ , which implies that  $\Gamma \curvearrowright (G, m_G)$  has local spectral gap.  $\square$

**1.2.2. Banach-Ruziewicz problem.** In [BISG], it is proved that the left translation action  $\Gamma \curvearrowright (G, m_G)$  having local spectral gap has many implications. Now some of these implications are mentioned.

**Theorem 3.** *Let  $\Gamma$  be a countable dense subgroup of a semisimple  $p$ -adic analytic group  $G$ . Suppose  $\text{Ad}(\Gamma)$  consists of matrices with algebraic entries in some  $\mathbb{Q}_p$ -basis of  $\text{Lie}(G)$ . Denote by  $\mathcal{C}(G)$  the family of measurable subsets  $A \subseteq G$  with compact closure.*

*Then up to a scalar there is a unique  $\Gamma$ -invariant, finitely additive measure  $\nu : \mathcal{C}(G) \rightarrow [0, \infty)$ .*

*Proof.* By [BISG, Theorem D], we know that, up to a multiplicative constant, the Haar measure of  $G$  is the unique finitely additive  $\Gamma$ -invariant measure defined on  $\mathcal{C}(G)$  if and only if the left translation action  $\Gamma \curvearrowright (G, m_G)$  has local spectral gap. Hence by Theorem 2 we get the desired result.  $\square$

**1.2.3. Orbit equivalence.** Another application of (local) spectral gap is in the theory of orbit equivalence of actions. There have been many breakthroughs in this subject in the past 15 years (see the surveys [Pop07, Fur11, Gab10]). Let us recall the notion of *orbit equivalence* for two left translation actions. Suppose  $\Gamma \subseteq G$  and  $\Lambda \subseteq H$  are dense subgroups. We say the left translation actions  $\Gamma \curvearrowright (G, m_G)$  and  $\Lambda \curvearrowright (H, m_H)$  are orbit equivalent if there exists a measure class preserving Borel isomorphism  $\theta : G \rightarrow H$  such that  $\theta(\Gamma g) = \Lambda \theta(g)$ , for  $m_G$ -almost every  $g \in G$ . Of course any action is orbit equivalent to an isomorphic copy of itself, i.e. if there is a topological isomorphism  $\delta : G \rightarrow H$  such that  $\delta(\Gamma) = \Lambda$ , then  $\Gamma \curvearrowright (G, m_G)$  and  $\Lambda \curvearrowright (H, m_H)$  are orbit equivalent. In such a case, we say the two actions are *conjugate*.

Two actions that are orbit equivalent can be far from being conjugate. In fact, surprisingly when  $\Gamma$  and  $\Lambda$  are infinite amenable groups, the mentioned actions are orbit equivalent [OW80, CFW81]. In the past decade it has been shown that in the presence of certain (local) spectral gap, however, the actions are *rigid*, i.e. orbit equivalence implies conjugation [Ioa14-a, Ioa14-b, BISG].

**Theorem 4.** *Let  $G$  be a semisimple  $p$ -adic analytic group, and  $\Gamma \subseteq G$  be a countable dense subgroup. Suppose  $\text{Ad}(\Gamma)$  consists of matrices with algebraic entries in some  $\mathbb{Q}_p$ -basis of  $\text{Lie}(G)$ . Let  $H$  be a locally compact, second countable, Hausdorff topological group, and  $\Lambda$  be a countable dense subgroup of  $H$ . Suppose  $H$  has a profinite open compact subgroup.*

*If  $\Gamma \curvearrowright (G, m_G)$  and  $\Lambda \curvearrowright (H, m_H)$  are orbit equivalent, then there are open compact subgroups  $G_0 \subseteq G$  and  $H_0 \subseteq H$  and a topological isomorphism  $\delta : G_0 \rightarrow H_0$  such that  $\delta(\Gamma \cap G_0) = \Lambda \cap H_0$ .*

*Proof.* Let  $G'_0 \subseteq G$  be a pro- $p$  open subgroup of  $G$ . As in the proof of Theorem 2, by Theorem 1, we have that  $\Gamma \cap G'_0 \curvearrowright (G'_0, m_{G'_0})$  has spectral gap.

Now let  $H'_0 \subseteq H$  be a profinite open subgroup. Since  $\Gamma \curvearrowright (G, m_G)$  and  $\Lambda \curvearrowright (H, m_H)$  are orbit equivalent,  $\Gamma \cap G'_0 \curvearrowright (G'_0, m_{G'_0})$  and  $\Lambda \cap H'_0 \curvearrowright (H'_0, m_{H'_0})$  are stably orbit equivalent. Hence by [Ioa14-a, Theorem A] there are open subgroups  $G_0$  and  $H_0$ , and a topological isomorphism  $\delta : G_0 \rightarrow H_0$  such that  $\delta(\Gamma \cap G_0) = \Lambda \cap H_0$ .  $\square$

**1.2.4. Super-approximation.** The connection between spectral gap and construction of expanders was first observed by Margulis [Mar73] where he proved that the family of Cayley graphs of finite quotients of a finitely generated group with property (T) is a family of expanders. Later due to works of several mathematicians [Sel65, Kaz67, BS91, Clo03, CU04], it was proved that the same holds for *congruence quotients* of an  $S$ -arithmetic group of a semisimple group. In the spirit of strong approximation, Lubotzky [Lub95] asked if this is an *algebraic* phenomenon or an *arithmetic* one.<sup>2</sup> More precisely, it was asked if the Cayley graphs of  $\text{SL}_2(\mathbb{f}_p)$  with respect to the generating set  $\left\{ \begin{bmatrix} 1 & \pm 3 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ \pm 3 & 1 \end{bmatrix} \right\}$  is a family of expanders. In [Gam02] it was proved that, if Hausdorff dimension of the limit set of  $\Gamma = \langle \Omega \rangle \subseteq \text{SL}_2(\mathbb{Z})$  is larger than  $5/6$ , then  $\{\text{Cay}(\pi_p(\Gamma), \pi_p(\Omega))\}_p$  is a family of expanders as  $p$  ranges over primes.

Later based on Helfgott's product theorem [Hel05], Bourgain and Gamburd in their seminal work [BG08-a] proved the same result for any finite symmetric subset  $\Omega \subseteq \text{SL}_2(\mathbb{Q})$  as long as  $\Gamma = \langle \Omega \rangle$  is Zariski-dense in  $\mathbb{SL}_2$ . Since then, based on their machinery and generalizations of Helfgott's work [Hel11, BGT11, PS], this result has been extended in several works [BG08-b, BG09, BGS10, Var12, BV12, SGV12].

As it was pointed out earlier, Theorem 1 implies that *super-approximation* holds for prime power modulus when the Zariski-closure of the group is semisimple. In a subsequent work based on Theorem 1, the author proves the best possible result for prime power modulus.

**Theorem 5.** *Let  $\Omega$  be a finite symmetric subset of  $\text{GL}_{n_0}(\mathbb{Q})$ ,  $\Gamma = \langle \Omega \rangle$ , and*

$$\mathcal{C}(\Gamma) := \{p \in V_f(\mathbb{Q}) \mid \Gamma \text{ is a bounded subgroup of } \text{GL}_{n_0}(\mathbb{Q}_p)\}.$$

---

<sup>2</sup>Following A. Kontorovich's suggestion, I call this phenomenon *super-approximation*. It is worth pointing out that this phenomenon has been called *superstrong approximation* (e.g. see [BO14]) by some authors.

Then  $\{\text{Cay}(\pi_{p^n}(\Gamma), \pi_{p^n}(\Omega))\}_{p \in \mathcal{C}(\Gamma), n \in \mathbb{Z}^+}$  is a family of expanders if and only if the connected component  $\mathbb{G}^\circ$  of the Zariski-closure  $\mathbb{G}$  of  $\Gamma$  is perfect, i.e.  $\mathbb{G}^\circ = [\mathbb{G}^\circ, \mathbb{G}^\circ]$ .

It is worth pointing out that, unlike Theorem 1, Theorem 5 does not hold for number fields (see [SGV12, Section 1.2]).

Let's also point out that Theorem 1 is stronger than the semisimple case of Theorem 5. Going to the Zariski closure of  $\Gamma$  in the Weil restriction of scalars  $R_{k/\mathbb{Q}}(\mathbb{G})$ , Theorem 5 implies that

$$\sup\{\lambda(\mathcal{P}_\Omega; \Gamma_{\mathfrak{p}}) \mid \mathfrak{p} \nmid N_{k/\mathbb{Q}}(a_0)\} < 1$$

if  $\Gamma \subseteq \text{GL}_{n_0}(\mathcal{O}_k[1/a_0])$  for some  $a_0 \in \mathcal{O}_k$ . So it does not tell us about places  $\mathfrak{p}$  that divide  $N_{k/\mathbb{Q}}(a_0)$  but not  $a_0$ . For instance, suppose  $\Gamma = \langle \Omega \rangle$  is a Zariski-dense subgroup of an arithmetic subgroup of  $\text{SL}_{n_0}(\mathbb{Q}_p)$  and suppose the trace field  $k$  of the arithmetic subgroup is not  $\mathbb{Q}$ . Then there is a place  $\mathfrak{p}$  of  $k$  which divides  $p$  and  $\Gamma$  is a bounded subgroup of  $\text{SL}_{n_0}(k_{\mathfrak{p}})$ , and Theorem 5 cannot give us a control on  $\lambda(\mathcal{P}_\Omega; \Gamma_{\mathfrak{p}})$ .

**1.3. Comparing with the previous related works.** There are two prior results related to Theorem 1. Both Bourgain-Gamburd [BG08-b, BG09] and Bourgain-Varjú [BV12] focus on the case of finitely generated, Zariski-dense subgroup  $\Gamma = \langle \Omega \rangle$  of  $\text{SL}_{n_0}(\mathbb{Z})$ . In [BG08-b, BG09], it is proved that  $\lambda(\mathcal{P}_\Omega; \Gamma_p) < \lambda(p) < 1$  if  $p$  is large enough depending on  $\Omega$ . In [BV12], using a different technique, it is proved that  $\lambda(\mathcal{P}_\Omega; \hat{\Gamma}) < 1$  where  $\hat{\Gamma}$  is the closure of  $\Gamma$  in  $\prod_{p \in V_f(\mathbb{Q})} \text{SL}_{n_0}(\mathbb{Z}_p)$ ; in particular,  $\sup\{\lambda(\mathcal{P}_\Omega; \Gamma_p) \mid p \in V_f(\mathbb{Q})\} < 1$ .

Both [BV12] and [BG09] rely on Archimedean dynamics. The former is based on [BFLM11] and the latter uses random-matrix theory in  $\text{SL}_{n_0}(\mathbb{Z})$ . And both of these works need the existence of proximal elements in the adjoint representation over  $\mathbb{R}$ . In particular, their arguments cannot be extended to the case where  $\mathbb{G}(\mathbb{R})$  is compact.

Our proof is inspired by the approach presented in [BG09]. Instead of random matrix theory, however, the main result of [SGV12] is used.

## ACKNOWLEDGMENTS.

I am in debt of Adrian Ioana for many insightful conversations about orbit equivalence rigidity, and in particular for telling me how to get such a result from the main theorem of this article. I would like to thank Kiran Kedlaya for the fruitful discussion about complete intersection varieties. I am thankful of Hee Oh for asking me about the  $p$ -adic version of local spectral gap after my talk at the MSRI.

## 2. PRELIMINARY RESULTS

**2.1. Spreading of weight under convolution, and  $l^2$ -flattening.** Let me start with the following (easy) lemma (see [BG09, Remark, page 1060]).

**Lemma 6.** *Let  $H$  be a group,  $\mu$  be a symmetric probability measure on  $H$ , and  $A$  be a symmetric subset of  $H$ . If  $l > l_0$  are two positive integers, then  $\mu^{(2l_0)}(A \cdot A) \geq \mu^{(l)}(A)^2$ .*

*Proof.* First we notice that, since  $\mu^{(l)}(A) = \sum_{h \in H} \mu^{(l-l_0)}(h) \mu^{(l_0)}(h^{-1}A)$ ,  $\mu^{(l)}(A) \leq \max_{h \in H} \mu^{(l_0)}(hA)$ . Now since  $A$  and  $\mu$  are symmetric, we also have that  $\mu^{(2l_0)}(A \cdot A) \geq \max_{h \in H} \mu^{(l_0)}(hA)^2$ .  $\square$

Let me recall the  $l^2$ -flattening phenomenon proved by Bourgain-Gamburd (see [Var12, Lemma 15] and [BG08-a]) which is based on the non-commutative version of Balog-Szemerédi-Gowers Theorem [Tao08].

**Lemma 7.** *Let  $H$  be a finite group and  $\mu$  be a probability measure on  $H$ . Let  $K$  be a positive number. If  $\|\mu * \mu\|_2 \geq \frac{1}{K} \|\mu\|_2$ , then there is a subset  $A$  of  $H$  with the following properties:*

- (1)  $\frac{1}{K^R \|\mu\|_2^2} \leq |A| \leq \frac{K^R}{\|\mu\|_2^2},$
- (2)  $|A \cdot A \cdot A| \leq K^R |A|,$
- (3)  $\min_{h \in A} (\tilde{\mu} * \mu)(h) \geq \frac{1}{K^R |A|},$  where  $\tilde{\mu}(h) = \mu(h^{-1})$  for any  $h \in H$ .

**2.2. Regularization.** In this section, we recall a regularization of a subset of a rooted regular tree due to Bourgain and Gamburd [BG09, Section A.3] (see Corollary 11). The proofs are included for the convenience of the reader.

**Definition 8.** (1) Let  $T = T_{k,n}$  be a rooted tree such that each vertex has  $k$  children and it has  $n$  generations (levels). The root is considered the zero-generation.  
 (2) For any  $0 \leq i \leq n$ , let  $T^{(i)}$  be the set of vertices in the  $i$ -th generation.  
 (3) For any  $0 \leq i \leq j \leq n$ , let  $\pi_{i,j} : T^{(j)} \rightarrow T^{(i)}$  be the projection map (which gives the “ancestor” of a vertex).  
 (4) For any vertex  $v \in T^{(i)}$ , let  $B(v) = \pi_{i,n}^{-1}(v) \subseteq T^{(n)}$  (the set of all the grand children of  $v$  after  $n - i$  generations).  
 (5) For a subset  $A$  of  $T^{(n)}$  and a vertex  $x \in T^{(i)}$ , let  $\deg_A(x) = |\pi_{i+1,n}(B(x) \cap A)|$ .

**Lemma 9.** Let  $k, n$  be two positive integers,  $T = T_{k,n}$  and  $A \subseteq T^{(n)}$ . Then there is  $k'$ , a power of 2, and  $A' \subseteq A$  such that

- (1) For every  $x \in \pi_{n-1,n}(A')$ , we have  $|B(x) \cap A'| = k'$ .
- (2)  $|A'| \geq |A|/(2 \log k)$ .

*Proof.* We have that

$$|A| = \sum_{x \in \pi_{n-1,n}(A)} |B(x) \cap A| = \sum_{i=0}^{\lfloor \log k \rfloor} \left( \sum_{\substack{x \in \pi_{n-1,n}(A) \\ 2^i \leq \deg_A(x) < 2^{i+1}}} \deg_A x \right).$$

So there are  $1 \leq i \leq \lfloor \log k \rfloor$  and

$$A' \subseteq \bigcup_{\substack{x \in \pi_{n-1,n}(A) \\ 2^i \leq \deg_A(x) < 2^{i+1}}} (B(x) \cap A)$$

such that  $k' = 2^i$  and  $A'$  satisfy the desired properties.  $\square$

**Lemma 10.** Let  $k, n$  be two positive integers,  $\varepsilon > 0$ ,  $T = T_{k,n}$  and  $A \subseteq T^{(n)}$ . Suppose that  $|A| \geq |T^{(n)}|^\varepsilon = k^{n\varepsilon}$  and  $k^{\varepsilon/4} > 2 \log k$  (i.e.  $k$  is “large enough” depending on  $\varepsilon$ ). Then there are  $B \subseteq A$  and a positive integer  $m \leq n(1 - \varepsilon/4)$  such that

- (1)  $\pi_{m,n}(B) = \{v\}$ .
- (2) For any  $m \leq l \leq n$ , we have that  $|\pi_{l,n}(B)| \geq k^{(l-m)\varepsilon/2}$ .

In particular, we have  $|B| \geq k^{n\varepsilon^2/8} = |T^{(n)}|^{\varepsilon^2/8}$ .

*Proof.* Repeated use of Lemma 9, we get a sequence of dyadic numbers  $k_0, k_1, \dots, k_{n-1}$  and a chain of subsets of  $A$

$$A_0 \subseteq A_1 \subseteq \dots \subseteq A_{n-1} \subseteq A_n = A,$$

such that

- (1) For any  $0 \leq i \leq n - 1$  and any  $x \in \pi_{i,n}(A_i)$ , we have  $\deg_{A_i}(x) = \dots = \deg_{A_{n-1}}(x) = k_i$ . And so  $|A_i| = |\pi_{j,n}(A_i)| \cdot k_j \cdot \dots \cdot k_{n-1}$  for any  $i \leq j \leq n - 1$ .

- (2) For any  $1 \leq i \leq n$ , we have  $|\pi_{i,n}(A_{i-1})| \geq |\pi_{i,n}(A_i)|/(2 \log k)$ . And so  $|A_{i-1}| \geq |A_i|/(2 \log k)$  and  $|A_i| \geq |A|/(2 \log k)^{n-i}$ .

In particular, we have  $|A_0| = k_0 \cdots k_{n-1} \geq |A|/(2 \log k)^n \geq k^{n\varepsilon}/k^{n\varepsilon/4} = k^{3n\varepsilon/4}$ . Let

$$m = \max\{i \mid 0 \leq i \leq n-1, \prod_{j=0}^{i-1} k_j < k^{i\varepsilon/2}\}.$$

Then for any  $x \in \pi_{m,n}(A_0)$  and any  $m+1 \leq l \leq n$  we have

$$|\pi_l(B(x) \cap A_0)| = \prod_{i=m}^{l-1} k_i = \left(\prod_{i=0}^{l-1} k_i\right) / \left(\prod_{i=0}^{m-1} k_i\right) \geq k^{l\varepsilon/2} / k^{m\varepsilon/2} = k^{(l-m)\varepsilon/2}.$$

On the other hand, we have

$$k^{3n\varepsilon/4} \leq |A_0| = \prod_{i=0}^{n-1} k_i = \prod_{i=0}^{m-1} k_i \cdot \prod_{i=m}^{n-1} k_i < k^{m\varepsilon/2} \cdot k^{n-m} = k^{n-m+m\varepsilon/2}.$$

And so  $m < n(1-3\varepsilon/4)/(1-\varepsilon/2) < n(1-\varepsilon/4)$ , which means  $B = B(x) \cap A_0$  for  $x \in \pi_{m,n}(A_0)$  and  $m$  satisfy the desired properties.  $\square$

**Corollary 11.** *Let  $k, n$  be two positive integers,  $\varepsilon > 0$ ,  $T = T_{k,n}$  and  $A \subseteq T^{(n)}$ . Suppose that  $|A| \geq |T^{(n)}|^\varepsilon = k^{n\varepsilon}$  and  $k^n \gg_\varepsilon 1$ . Then there are  $B \subseteq A$  and a positive integer  $m \leq n(1-\varepsilon/4)$  such that*

- (1)  $\pi_{m,n}(B) = \{v\}$ .
- (2) For any  $m \leq l \leq n$ , we have that  $|\pi_{l,n}(B)| \gg_\varepsilon k^{(l-m)\varepsilon/4}$ .

In particular, we have  $|B| \geq k^{n\varepsilon^2/32} = |T^{(n)}|^{\varepsilon^2/32}$ .

*Proof.* Let  $K(\varepsilon)$  be the smallest positive real number such that  $K(\varepsilon)^{\varepsilon/4} \geq 2 \log K(\varepsilon)$ . And let  $s$  be the smallest positive integer such that  $k^s \geq K(\varepsilon)$ . Now let us consider  $T' := T_{k^l, \lfloor n/l \rfloor}$  and identify  $\pi_{s \lfloor n/s \rfloor, n}(A)$  with a subset  $A'$  of  $T'^{(\lfloor n/s \rfloor)}$ . We notice that  $|A'| \geq K(\varepsilon)^{-1} |A| \geq K(\varepsilon)^{-1} k^{n\varepsilon} \geq k^{n\varepsilon/2}$  if  $k^n \geq K(\varepsilon)^{2/\varepsilon}$ . So by Lemma 10 there are  $B' \subseteq A'$  and a positive integer  $m' \leq \lfloor n/s \rfloor (1-\varepsilon/8)$  such that

- (1)  $\pi_{sm', s \lfloor n/s \rfloor}(B') = \{v\}$ .
- (2) For any  $m' \leq l \leq \lfloor n/s \rfloor$ , we have that  $|\pi_{sl, s \lfloor n/s \rfloor}(B)| \geq k^{s(l-m')\varepsilon/4}$ .

Let  $B \subseteq A$  be such that  $\pi_{s \lfloor n/s \rfloor, n}(B) = B'$  and let  $m = sm'$ . Then for any positive integer  $l$  between  $m$  and  $n$  we have

$$|\pi_{l,n}(B)| \geq K(\varepsilon)^{-1} |\pi_{s \lfloor l/s \rfloor, s \lfloor n/s \rfloor}(B')| \geq K(\varepsilon)^{-1} k^{s(\lfloor l/s \rfloor - m')\varepsilon/4} \geq K(\varepsilon)^{-2} k^{(l-m)\varepsilon/4}.$$

In particular,  $|B| \geq K(\varepsilon)^{-2} k^{n\varepsilon^2/16} \geq k^{n\varepsilon^2/32}$  if  $k^n \geq K(\varepsilon)^{\max\{64/\varepsilon^2, 2/\varepsilon\}}$ .  $\square$

**2.3. Reduction to the connected, simply-connected case.** Let  $\Gamma^\circ = \Gamma \cap \mathbb{G}^\circ$ . So  $\Gamma^\circ$  is a Zariski-dense subgroup of  $\mathbb{G}^\circ$  which is a finite-index normal subgroup of  $\Gamma$ . The following lemma and corollary are crucial in the reduction to a connected, simply-connected group.

**Lemma 12.** *Let  $\Gamma$  be a finitely generated group generated by a symmetric set  $\Omega$ , and  $\Lambda$  be a finite index normal subgroup of  $\Gamma$ . Let  $\{N_i\}$  be a family of finite index normal subgroups of  $\Gamma$ . Then  $\Gamma$  has property  $(\tau)$  with respect to  $\{N_i\}$  if and only if  $\Lambda$  has property  $(\tau)$  with respect to  $\{N_i \cap \Lambda\}$ . (See [Lub94, Chapter 4.3])*

*Proof.* Suppose  $S = \{s_1, \dots, s_k\}$  is a symmetric generating set of  $\Gamma$  and at the same time  $\Gamma = \bigcup_{i=1}^k s_i \Lambda$ . So for any  $1 \leq i, j \leq k$  there is  $1 \leq l = l(i, j) \leq k$  such that  $s_i \Lambda = s_j s_l \Lambda$ . Let  $s'_{i,j} := s_{l(i,j)}^{-1} s_i s_j \in \Lambda$ . Then we claim that  $\Lambda$  is generated by  $S' := \{s'_{i,j}\} \cup (S \cap \Lambda)$ . Let  $\Lambda_1$  be the group generated by  $S'$ . Clearly it is

a subgroup of  $\Lambda$ . By the definition of  $s'_{i,j}$  we have that  $s_{l(i,j)}\Lambda_1 = s_i s_j \Lambda_1$ . And so  $\Gamma = \bigcup_{i=1}^k s_i \Lambda_1$  since  $S$  generates  $\Gamma$  and is symmetric. Therefore we get that  $\Lambda_1 = \Lambda$ .

Assume that  $\Gamma$  has property( $\tau$ ) with respect to  $\{N_i\}$ . So there is  $\varepsilon > 0$  such that for any  $i$  and any unit vector  $u$  of

$$l_0^2(\Gamma/N_i) := \{f : \Gamma/N_i \rightarrow \mathbb{C} \mid \sum_{\bar{\gamma} \in \Gamma/N_i} f(\bar{\gamma}) = 0\},$$

we have

$$(1) \quad \max_{s_i \in S} \{\|s_i u - u\|\} > \varepsilon.$$

Now assume that  $v$  is a unit vector in an irreducible non-trivial representation  $\rho : \Lambda/(N_i \cap \Lambda) \rightarrow \text{GL}(V)$  which is an  $\varepsilon'$ -almost invariant vector with respect to  $S'$ , i.e. for any  $s' \in S'$  we have

$$\|\rho(s')(v) - v\| < \varepsilon'.$$

By Frobenius reciprocity,  $\tilde{\rho} := \text{Ind}_{\Lambda/(N_i \cap \Lambda)}^{\Gamma/N_i} \rho$  is a subrepresentation of  $l_0^2(\Gamma/N_i)$ . Let  $\{s_{i'}\}_{i' \in I} \subseteq S$  be a set which induces (distinct) coset representatives of  $\Lambda N_i/N_i$  in  $\Gamma/N_i$ . Then  $\tilde{\rho}$  can be described as follows:  $W := \bigoplus_{i' \in I} s_{i'} V$  (where  $s_{i'} V$  are orthogonal copies of  $V$ ) and, for any  $\gamma \in \Gamma$ , we have

$$\tilde{\rho}(\gamma)(\sum_{i' \in I} s_{i'} x_{i'}) = \sum_{i' \in I} s_{l'_\gamma(i')} \rho(s_{l'_\gamma(i')}^{-1} \gamma s_{i'})(x_{i'}),$$

where  $l'_\gamma(i')$  is the unique element of  $I$  such that  $s_{l'_\gamma(i')} \Lambda N_i = \gamma s_{i'} \Lambda N_i$ .

Notice that for any  $i', j$  we have  $s_{l'_{s_{i'}}(j)}^{-1} s_{i'} s_j$  is a multiple of at most 5 elements of  $S'$ , and so we have

$$\|\rho(s_{l'_{s_{i'}}(j)}^{-1} s_{i'} s_j)(v) - v\| < 5\varepsilon'.$$

Hence, for any  $1 \leq i' \leq k$ , we have

$$\begin{aligned} \|\tilde{\rho}(s_{i'})\left(\sum_{j \in I} s_j v\right) - \sum_{j \in I} s_j v\| &= \left\| \sum_{j \in I} s_{l'_{s_{i'}}(j)} \rho(s_{l'_{s_{i'}}(j)}^{-1} s_{i'} s_j)(v) - \sum_{j \in I} s_j v \right\| \\ &\leq 5|\Gamma/\Lambda|\varepsilon' + \left\| \sum_{j \in I} s_{l'_{s_{i'}}(j)} v - \sum_{j \in I} s_j v \right\| = 5|\Gamma/\Lambda|\varepsilon'. \end{aligned}$$

So by (1) we have that  $\varepsilon < 5|\Gamma/\Lambda|\varepsilon'$ . Thus no non-trivial irreducible representation of  $\Lambda/(N_i \cap \Lambda)$  has an  $\varepsilon/(5|\Gamma/\Lambda|)$ -almost invariant vector with respect to  $S'$ , which proves that  $\Lambda$  has property( $\tau$ ) with respect to  $\{N_i \cap \Lambda\}$ .

Now assume that  $\Lambda$  has property( $\tau$ ) with respect to  $N_i \cap \Lambda$ . So there is  $\varepsilon > 0$  such that for any unit vector  $u \in l_0^2(\Lambda/(\Lambda \cap N_i))$  we have

$$(2) \quad \max_{s' \in S'} \|s' u - u\| > \varepsilon.$$

Let  $\rho$  be an irreducible representation of  $\Gamma/N_i$  which does not factor through  $\Gamma/\Lambda$ . Suppose that  $v$  is a unit vector in  $V_\rho$  which is  $\varepsilon'$ -almost invariant vector with respect to  $S$ , i.e.

$$\|\rho(s)(v) - v\| \leq \varepsilon',$$

for any  $s \in S$ . Therefore for any  $s' \in S'$  we have

$$\|\rho(s')(v) - v\| \leq 3\varepsilon'.$$

By Frobenius reciprocity and, since  $\rho$  does not factor through  $\Gamma/\Lambda$ , the restriction of  $\rho$  to  $\Lambda/(\Lambda \cap N_i)$  is a subrepresentation of  $l_0^2(\Lambda/(\Lambda \cap N_i))$ . Thus by (2) we have  $\varepsilon < 3\varepsilon'$ , which implies that any non-trivial representation of  $\Gamma/N_i$  has no  $\varepsilon''$ -almost invariant vector with respect to  $S$  for some  $0 < \varepsilon'' < \varepsilon/3$ .  $\square$



**Corollary 13.** *Let  $\Gamma$  be a finitely generated group and  $\Omega$  be a symmetric finite generating set of  $\Gamma$ . Assume  $\Lambda$  be a finite-index subgroup of  $\Gamma$ . Then  $\Lambda$  has a finite symmetric generating set  $\Omega'$ , and for any infinite set  $\{N_i\}$  of normal finite index subgroups of  $\Gamma$ ,  $\{\text{Cay}(\Gamma/N_i, \pi_{N_i}(\Omega))\}_i$  is a family of expanders if and only if  $\{\text{Cay}(\Lambda/(N_i \cap \Lambda), \pi_{N_i \cap \Lambda}(\Omega'))\}_i$  is a family of expanders.*

*Proof.* This is a direct corollary of Lemma 12 and [Lub94, Theorem 4.3.2].  $\square$

By Corollary 13 we have that  $\Gamma^\circ$  has a symmetric finite generating set  $\Omega^\circ$  and  $\{\text{Cay}(\pi_q(\Gamma), \pi_q(\Omega))\}_{q \in \mathcal{C}}$  is a family of expanders if and only if  $\{\text{Cay}(\pi_q(\Gamma^\circ), \pi_q(\Omega^\circ))\}_{q \in \mathcal{C}}$  is a family of expanders for any infinite set  $\mathcal{C}$  of positive integers. So from this point on we can assume that  $\mathbb{G}$  is a Zariski-connected semisimple group. Let  $\tilde{\mathbb{G}}$  be the simply-connected form of  $\mathbb{G}$  that is defined over  $k$ . Let  $\iota : \tilde{\mathbb{G}} \rightarrow \mathbb{G}$  be the  $k$ -covering map,  $\tilde{\Lambda} := \iota^{-1}(\Gamma) \cap \tilde{\mathbb{G}}(k)$ , and  $\Lambda := \iota(\tilde{\Lambda})$ . By a similar argument as in [SGS13, Lemma 24] we have that  $\Lambda$  is a normal finite-index subgroup of  $\Gamma$ . Hence again by Corollary 13 without loss of generality we can assume that  $\Gamma = \Lambda$ .

On the other hand,  $\iota$  induces continuous homomorphism with finite kernel from  $\tilde{\mathbb{G}}(k_{\mathfrak{p}})$  to  $\mathbb{G}(k_{\mathfrak{p}})$ . So after fixing a  $k$ -embedding  $\tilde{\mathbb{G}} \xrightarrow{f} \mathbb{G}\mathbb{L}_n$  and passing to a finite-index subgroup (as we are allowed by Corollary 13), if needed, we can assume that  $f(\tilde{\Lambda}) \subseteq \mathbb{G}\mathbb{L}_n(\mathcal{O}_k(S))$ . And there is  $(m_{\mathfrak{p}}) \in \bigoplus_{\mathfrak{p} \in V_f(k)} \mathbb{Z}$  such that for any  $\mathfrak{p} \in V_f(k)$  (where  $V_f(k)$  is the set of all finite places of  $k$ ),

$$|f(\tilde{\lambda}) - 1|_{\mathfrak{p}} \leq |N_{k/\mathbb{Q}}(\mathfrak{p})|^{m_{\mathfrak{p}}} |\tilde{\lambda} - 1|_{\mathfrak{p}}.$$

Hence  $f$  induces an epimorphism from  $\pi_{\mathfrak{p}^n}(\tilde{\Lambda})$  onto  $\pi_{\mathfrak{p}^n - m_{\mathfrak{p}}}(\Gamma)$ . So  $\{\text{Cay}(\pi_{\mathfrak{p}^n}(\tilde{\Lambda}), \pi_{\mathfrak{p}^n}(\tilde{\Omega}))\}_{\mathfrak{p} \notin S, n \in \mathbb{Z}^+}$  is a family of expanders if and only if  $\{\text{Cay}(\pi_{\mathfrak{p}^n}(\Gamma), \pi_{\mathfrak{p}^n}(\Omega))\}_{\mathfrak{p} \notin S, n \in \mathbb{Z}^+}$  is a family of expanders. This implies that without loss of generality we can assume  $\mathbb{G}$  is simply connected. So we have proved that:

**Lemma 14.** *It is enough to prove Theorem 1 for a subgroup  $\Gamma = \langle \Omega \rangle$  of  $\mathbb{G}\mathbb{L}_{n_0}(\mathcal{O}_k(S))$  under the assumptions that its Zariski-closure is Zariski-connected, simply-connected, semisimple  $k$ -group.*

**2.4. Strong approximation and the  $\mathfrak{p}$ -adic closures of  $\Gamma$ .** Here using strong approximation [Nor89, Theorem 5.4], we describe structure of the closure  $\Gamma_{\mathfrak{p}}$  of  $\Gamma$  in  $\mathbb{G}\mathbb{L}_{n_0}(\mathcal{O}_{\mathfrak{p}})$  for any  $\mathfrak{p} \notin S$ . Consider  $\Gamma$  as a subgroup of  $R_{k/\mathbb{Q}}(\mathbb{G})(\mathbb{Q})$  and let  $\mathbb{G}_1$  be its Zariski-closure. Since  $R_{k/\mathbb{Q}}(\mathbb{G})$  is isomorphic to  $\prod_{\sigma \in \text{hom}(k, \overline{\mathbb{Q}})} \mathbb{G}^{\sigma}$  over  $k$  and the projection of  $\Gamma$  to each factor is Zariski-dense,  $\mathbb{G}_1$  is a semisimple  $\mathbb{Q}$ -group. Since  $\mathbb{G}$  is simply-connected, so is  $\mathbb{G}_1$ . Let

$$S_0 := \{p \in V_f(\mathbb{Q}) \mid \mathfrak{p} | p \text{ for some } \mathfrak{p} \in S\}.$$

Let us fix a  $k$ -embedding of  $\mathbb{G}$ , a  $\mathbb{Z}$ -basis of  $\mathcal{O}_k$ , and fix the induced  $\mathbb{Q}$ -embedding of  $R_{k/\mathbb{Q}}(\mathbb{G})$  and get a  $\mathbb{Q}$ -embedding of  $\mathbb{G}_1$  in  $\mathbb{G}\mathbb{L}_{n_1}$ . Then  $\Gamma \subseteq \mathbb{G}\mathbb{L}_{n_1}(\mathbb{Z}_{S_0})$ . Hence by Nori's strong-approximation, after going to a finite index subgroup if necessary (it is allowed by Corollary 13), we can assume the following:

- (1) The closure  $\hat{\Gamma}$  of  $\Gamma$  in  $\prod_{p \notin S_0} \mathbb{G}_1(\mathbb{Z}_p)$  is an open compact subgroup.
- (2)  $\hat{\Gamma} = \prod_{p \notin S_0} K_p$  where  $K_p$  is an open compact subgroup of  $\mathbb{G}_1(\mathbb{Q}_p)$ .
- (3) For large enough  $p$ ,  $K_p$  is a hyperspecial parahoric.
- (4) If  $K_p$  is not a hyperspecial parahoric, then it is a uniformly powerful pro- $p$  group (see [DDMS99] for the definition of a uniform pro- $p$  group).
- (5) For any  $p \notin S_0$ , either  $\pi_p(\Gamma)$  is perfect or it is trivial. And  $\Gamma_{\mathfrak{p}}$  is a quotient of  $K_p$ .

Since  $\Gamma_{\mathfrak{p}}$  is a quotient of  $K_p$  for any  $p \notin S_0$  and  $\mathfrak{p} | p$ , we have that  $\lambda(\mathcal{P}_{\Omega}; K_p) \geq \lambda(\mathcal{P}_{\Omega}; \Gamma_{\mathfrak{p}})$ . Let

$$\tilde{S} := \{\mathfrak{p} \in V_f(k) \mid \mathfrak{p} \notin S, \mathfrak{p} | p \text{ for some } p \in S_0\}.$$

Hence proving Theorem 1 splits into two parts: proving a uniform spectral gap for  $k = \mathbb{Q}$  and proving a spectral gap for a fixed  $\mathfrak{p} \in \mathcal{C}$ .

For any  $\mathfrak{p} \in \mathcal{C}$ , by assumption, the closure  $\Gamma_{\mathfrak{p}}$  of  $\Gamma$  in  $\mathbb{G}(k_{\mathfrak{p}})$  is a compact group. Going to a finite-index subgroup if necessary (again we are allowed by Corollary 13), we can assume that  $\Gamma_{\mathfrak{p}}$  is a uniformly powerful pro- $p$  group, and the logarithmic map induces a bijection between  $\Gamma_{\mathfrak{p}}$  and a Lie  $\mathbb{Z}_p$ -subalgebra  $\mathfrak{g}_{\mathfrak{p}}$  of  $\text{Lie}(\mathbb{G})(k_{\mathfrak{p}})$ . Since  $\Gamma$  is Zariski-dense in  $\mathbb{G}$ , the  $k_{\mathfrak{p}}$ -span of  $\mathfrak{g}_{\mathfrak{p}}$  is the entire  $\text{Lie}(\mathbb{G})(k_{\mathfrak{p}})$ . And so  $\mathfrak{g}_{\mathfrak{p}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$  is a semisimple Lie algebra. Hence the Zariski-closure  $\overline{\mathbb{G}}_{1,\mathfrak{p}}$  of  $\Gamma_{\mathfrak{p}}$  in  $R_{k_{\mathfrak{p}}/\mathbb{Q}_p}(\mathbb{G} \times_k k_{\mathfrak{p}})$  is a semisimple  $\mathbb{Q}_p$ -group and  $\Gamma_{\mathfrak{p}}$  is an open compact subgroup of  $\overline{\mathbb{G}}_{1,\mathfrak{p}}(\mathbb{Q}_p)$ .

Without loss of generality we can and will assume that  $k$  is a Galois extension of  $\mathbb{Q}$ . Let  $\text{Gal}(k/\mathbb{Q})$  be the Galois group, and  $\text{Gal}(k/\mathbb{Q}; \mathfrak{p}) := \{\sigma \in \text{Gal}(k/\mathbb{Q}) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$  be the decomposition group. Let  $k(\mathfrak{p})$  be the subfield of fixed points of  $\text{Gal}(k/\mathbb{Q}; \mathfrak{p})$ . It is well-known that the restriction map induces an isomorphism between the Galois group  $\text{Gal}(k_{\mathfrak{p}}/\mathbb{Q}_p)$  and the decomposition group  $\text{Gal}(k/\mathbb{Q}; \mathfrak{p})$ . In particular, the natural embedding of  $k$  in  $k_{\mathfrak{p}}$  sends  $k(\mathfrak{p})$  to  $\mathbb{Q}_p$ . And so we have a (natural)  $\mathbb{Q}_p$ -isomorphism

$$(3) \quad R_{k_{\mathfrak{p}}/\mathbb{Q}_p}(\mathbb{G} \times_k k_{\mathfrak{p}}) \simeq R_{k/k(\mathfrak{p})}(\mathbb{G}) \times_{k(\mathfrak{p})} \mathbb{Q}_p.$$

There is a natural projection  $\text{Pr}_{\mathfrak{p}}$  from  $R_{k/\mathbb{Q}}(\mathbb{G})$  to  $R_{k/k(\mathfrak{p})}(\mathbb{G})$  that is defined over  $k(\mathfrak{p})$ . Let  $\mathbb{G}_{1,\mathfrak{p}} := \text{Pr}_{\mathfrak{p}}(\mathbb{G}_1)$ . By (3), we get the following natural  $\mathbb{Q}_p$ -isomorphism

$$(4) \quad \overline{\mathbb{G}}_{1,\mathfrak{p}} \simeq \mathbb{G}_{1,\mathfrak{p}} \times_{k(\mathfrak{p})} \mathbb{Q}_p.$$

Let's summarize what we have proved in the following Lemma.

**Lemma 15.** *Let  $k$  be a finite Galois extension of  $\mathbb{Q}$ . Let  $\Gamma$  be a finitely generated subgroup of  $\text{GL}_{n_0}(k)$ . Suppose the Zariski-closure  $\mathbb{G}$  of  $\Gamma$  is a connected, simply-connected semisimple group. Then for any*

$$\mathfrak{p} \in \mathcal{C}(\Gamma) := \{\mathfrak{p} \in V_f(k) \mid \Gamma \text{ is a bounded subgroup of } \mathbb{G}(k_{\mathfrak{p}})\}$$

*there is a subfield  $k(\mathfrak{p})$  of  $k$ , a connected, simply connected, semisimple  $k(\mathfrak{p})$ -group  $\mathbb{G}_{1,\mathfrak{p}}$  such that*

- (1) *Under the natural embedding of  $k$  into  $k_{\mathfrak{p}}$ ,  $k(\mathfrak{p})$  is mapped to  $\mathbb{Q}_p$ .*
- (2)  *$\Gamma_{\mathfrak{p}}$  is an open compact subgroup of  $\mathbb{G}_{1,\mathfrak{p}}(\mathbb{Q}_p)$ .*
- (3)  *$R_{k(\mathfrak{p})/\mathbb{Q}}(\mathbb{G}_{1,\mathfrak{p}})$  is naturally isomorphic to the Zariski-closure  $\mathbb{G}_1$  of  $\Gamma$  in  $R_{k/\mathbb{Q}}(\mathbb{G})$ .*

An important application of strong approximation and the above discussion is the following:

**Lemma 16.** *Let  $\Omega \subseteq \text{GL}_{n_0}(k)$  be a finite symmetric set. Suppose the Zariski-closure  $\mathbb{G}$  of the group  $\Gamma$  generated by  $\Omega$  is a Zariski-connected, simply-connected, semisimple group. Let*

$$\mathcal{C}(\Gamma) := \{\mathfrak{p} \in V_f(k) \mid \Gamma \text{ is a bounded subgroup of } \mathbb{G}(k_{\mathfrak{p}})\}.$$

*Suppose  $\Lambda$  is a finitely generated subgroup of  $\Gamma$  which is Zariski-dense in  $\Gamma$  considered as a subgroup of  $R_{k/\mathbb{Q}}(\mathbb{G})(\mathbb{Q})$ . Then for any  $\mathfrak{p} \in \mathcal{C}(\Gamma)$  we have that  $\Lambda_{\mathfrak{p}}$  is a finite-index subgroup of  $\Gamma_{\mathfrak{p}}$ , where  $\Gamma_{\mathfrak{p}}$  (resp.  $\Lambda_{\mathfrak{p}}$ ) is the closure of  $\Gamma$  (resp.  $\Lambda$ ) in  $\mathbb{G}(k_{\mathfrak{p}})$ . Furthermore for almost all  $\mathfrak{p} \in \mathcal{C}(\Gamma)$  we have  $\Gamma_{\mathfrak{p}} = \Lambda_{\mathfrak{p}}$ .*

*Proof.* Since  $\Gamma$  is finitely generated,  $S_0 := V_f(k) \setminus \mathcal{C}(\Gamma)$  is a finite set. Passing to a finite-index subgroup of  $\Gamma$ , if needed, we can assume that  $\Gamma \subseteq \text{GL}_{n_0}(\mathcal{O}_k(S_0))$ . As before, let  $\overline{S}_0 := \{p \in V_f(\mathbb{Q}) \mid p|p \text{ for some } p \in S_0\}$ . Then  $\Gamma \subseteq R_{\mathcal{O}_k/\mathbb{Z}}(\text{GL}_{n_0})(\mathbb{Z}_{\overline{S}_0})$ . By strong approximation, the closure  $\widehat{\Lambda}$  of  $\Lambda$  in

$$\prod_{p \in V_f(\mathbb{Q}) \setminus \overline{S}_0} \mathbb{G}_1(\mathbb{Z}_p)$$

is an open subgroup. Hence  $\widehat{\Lambda}$  is a finite-index subgroup of  $\widehat{\Gamma}$ , which proves that for almost all  $\mathfrak{p}$  we have  $\Gamma_{\mathfrak{p}} = \Lambda_{\mathfrak{p}}$ .

For a given  $\mathfrak{p}$ , we know that  $\Lambda_{\mathfrak{p}}$  is an open subgroup of a  $p$ -adic analytic group. And so it is open in the  $\mathbb{Q}_p$ -points of the Zariski-closure of  $R_{k_{\mathfrak{p}}/\mathbb{Q}_p}(\mathbb{G})(\mathbb{Q}_p)$ . Since  $\Lambda$  is Zariski-dense in  $\mathbb{G}_1$  (when considered as a subgroup of  $R_{k/\mathbb{Q}}(\mathbb{G})(\mathbb{Q})$ ), by the above discussion its Zariski-closure as a subgroup of  $R_{k_{\mathfrak{p}}/\mathbb{Q}_p}(\mathbb{G})(\mathbb{Q}_p)$  is  $\text{Pr}_{\mathfrak{p}}(\mathbb{G}_1) \times_{k(\mathfrak{p})} \mathbb{Q}_p$ . This implies that  $\Lambda_{\mathfrak{p}}$  is an open subgroup of  $\Gamma_{\mathfrak{p}}$ .  $\square$

**2.5. Ping-pong players and the main result of [SGV12].** One of the essential ingredients of this work is the following case of [SGV12, Corollary 6].

**Theorem 17.** *In the setting of Theorem 1,  $\{\text{Cay}(\pi_{\mathfrak{p}}(\Gamma), \pi_{\mathfrak{p}}(\Omega))\}_{\mathfrak{p} \in \mathcal{C}}$  is a family of expanders.*

As in [SGV12], first we change the probability law of the random-walk. The following can be deduced as a byproduct of the proof of [SGV12, Proposition 6].

**Proposition 18.** *In the setting of Theorem 1, let  $\mathbb{G}_1$  be the Zariski-closure of  $\Gamma$  in  $R_{k/\mathbb{Q}}(\mathbb{G})$ . Then there are a finite subset  $\overline{\Omega'}$  of  $\Gamma$  and  $\delta_0 > 0$  and  $l_0$  (which depend on  $\Omega$ ) such that  $\overline{\Omega'}$  freely generates a Zariski-dense subgroup of  $\mathbb{G}_1$  and*

$$(5) \quad \mathcal{P}_{\Omega'}^{(l)}(\mathbb{H}) \leq e^{-\delta_0 l}$$

for any proper subgroup  $\mathbb{H}$  of  $\mathbb{G}_1$  and  $l \geq l_0$ , where  $\Omega' = \overline{\Omega'} \cup \overline{\Omega'}^{-1}$ .

Furthermore if  $\mathbb{G}_1^{(i)}$  are  $\mathbb{Q}$ -almost simple factors of  $\mathbb{G}_1$ , then we can also assume that  $\text{pr}_i(\text{Ad}(\overline{\Omega'}))$  freely generates a Zariski-dense subgroup of  $\text{Ad}(\mathbb{G}_1^{(i)})$ , where  $\text{pr}_i : \text{Ad}(\mathbb{G}) \rightarrow \text{Ad}(\mathbb{G}_1^{(i)})$  are the projection maps. In particular,  $\ker(\text{pr}_i \circ \text{Ad}) \cap \langle \overline{\Omega'} \rangle = \{1\}$ .

*Proof.* This is essentially proved in [SGV12, Proposition 17, Proposition 20, Proposition 7] (for more general groups). Let us quickly give the outline of the argument for the semisimple case.

It is enough to find such upper bound for subgroups  $\mathbb{H}$  that are defined over  $\mathbb{Q}$  as  $\Gamma \subseteq \mathbb{G}_1(\mathbb{Q})$ . Since the order of a finite subgroup of  $\text{GL}_{n_0}(k)$  has an upper bound in terms of the degree of  $k$  and  $n_0$  without loss of generality we can assume that  $\dim \mathbb{H} \neq 0$ .

If the Zariski-connected component  $\mathbb{H}^\circ$  of  $\mathbb{H}$  is not normal, then  $\wedge^{\dim \mathbb{H}} \text{Lie}(\mathbb{H})$  is  $\mathbb{H}$ -invariant, but not  $\mathbb{G}_1$ -invariant. If  $\mathbb{H}^\circ$  is normal, then we have a good understanding of the structure of  $\mathbb{H}$  which gives us a subspace of  $\text{Lie}(\mathbb{G}_1)$  that is  $\mathbb{H}$ -invariant, but not  $\mathbb{G}_1$ -invariant. Then we consider the irreducible sub-representations of  $\wedge \text{Lie}(\mathbb{G})$  that factor through  $\mathbb{G}_1^{(i)}$  and find a subset  $\overline{\Omega'}$  that its elements play simultaneously ping-pong on the projective spaces of the above irreducible representations over appropriate local fields (see [SGV12, Lemma 19, Proposition 21]). So by [SGV12, Proposition 20], there are  $l_0$  and  $c > 0$  such that  $\overline{\Omega'}$  freely generates a subgroup of  $\Gamma$  and

$$|B_l(\overline{\Omega'}) \cap \mathbb{H}| < |B_l(\overline{\Omega'})|^{1-c},$$

for any Zariski-connected subgroup  $\mathbb{H}$  and any  $l \geq l_0$ , where  $B_l(\overline{\Omega'})$  is the set of reduced words over  $\overline{\Omega'}$  of length at most  $l$ . Now using a result of Kesten [Kes59, Theorem 3] and Cauchy-Schwartz as in the proof of [SGV12, Proposition 6], one can finish the proof.

Furthermore by the virtue of the proof of [SGV12, Proposition 21] (where the ping-pong players are constructed) we can make sure that  $\text{pr}_i(\text{Ad}(\overline{\Omega'}))$  freely generates a subgroup of  $\text{Ad}(\mathbb{G}_1^{(i)})$ .  $\square$

**Lemma 19.** *Let  $\Omega$  be a finite symmetric subset of  $\text{GL}_{n_0}(k)$  and  $\Gamma = \langle \Omega \rangle$ . Assume the Zariski-closure  $\mathbb{G}$  of  $\Gamma$  is a connected, simply connected, semisimple  $k$ -group. Suppose  $\Omega' \subseteq \Gamma$  is a finite symmetric set which generates a Zariski-dense subgroup  $\Lambda$  of  $\Gamma$  viewed as a subgroup of  $R_{k/\mathbb{Q}}(\mathbb{G})(\mathbb{Q})$ . Let*

$$\mathcal{C}(\Gamma) := \{\mathfrak{p} \in V_f(k) \mid \Gamma \text{ is a bounded subgroup of } \mathbb{G}(k_{\mathfrak{p}})\}.$$

*Then if  $\sup\{\lambda(\mathcal{P}_{\Omega'}; \Lambda_{\mathfrak{p}}) \mid \mathfrak{p} \in \mathcal{C}(\Gamma)\} < 1$ , then  $\sup\{\lambda(\mathcal{P}_{\Omega}; \Gamma_{\mathfrak{p}}) \mid \mathfrak{p} \in \mathcal{C}(\Gamma)\} < 1$ .*

*Proof.* Suppose the contrary. So there are  $\mathfrak{p}_i \in \mathcal{C}(\Gamma)$ , non-trivial unitary irreducible representations  $\rho_i : \Gamma_{\mathfrak{p}} \rightarrow \mathcal{U}(V_i)$ , and unit vectors  $v_i \in V_i$  such that

$$(6) \quad \|\rho_i(\gamma)(v_i) - v_i\| \rightarrow 0$$

for any  $\gamma \in \Omega$ . Since  $\Gamma = \langle \Omega \rangle$ , for any  $\gamma \in \Gamma$ , Equation (6) holds. In particular,  $\{v_i\}$  are almost invariant under  $\Omega'$ . Since  $\sup\{\lambda(\mathcal{P}_{\Omega'}; \Lambda_{\mathfrak{p}}) \mid \mathfrak{p} \in \mathcal{C}(\Gamma)\} < 1$ , a sequence of almost invariant functions are invariant from

some point on. Which means the restriction of  $\rho_i$  to  $\Lambda_{\mathfrak{p}_i}$  has a fixed point. Hence  $\Lambda_{\mathfrak{p}_i} \neq \Gamma_{\mathfrak{p}_i}$ . By Lemma 19, there are only finitely many of such  $\mathfrak{p}_i$ . So passing to a subsequence, if needed, we can assume that  $\mathfrak{p}_i = \mathfrak{p}$  is fixed. Again by Lemma 19,  $\Lambda_{\mathfrak{p}}$  is a finite index subgroup of  $\Gamma_{\mathfrak{p}}$ . So by Frobenius reciprocity, there are only finitely many irreducible representations of  $\Gamma_{\mathfrak{p}}$  whose restriction to  $\Lambda_{\mathfrak{p}}$  is trivial. Hence passing to a subsequence, if needed, we can assume that  $\rho_i = \rho$  is a fixed representation. This is clearly impossible as  $\rho$  is a finite-dimensional non-trivial irreducible representation of  $\Gamma_{\mathfrak{p}}$  and a such a representation cannot have almost invariant vectors.  $\square$

**2.6. Summary of the initial reductions.** In this short section, for the convenience of the reader, all the reductions is summarized. It is enough to prove Theorem 1 under the following conditions:

- (1) The Zariski-closure  $\mathbb{G}$  of  $\Gamma$  as a subgroup of  $\mathrm{GL}_{n_0}(k)$  is a *Zariski-connected, simply-connected, semisimple  $k$ -group*.
- (2)  $\Omega = \overline{\Omega} \cup \overline{\Omega}^{-1}$  is a subset of  $\mathrm{GL}_{n_0}(\mathcal{O}_k(S))$ , where  $S$  is a finite subset of  $V_f(k)$ . And, for any  $\mathfrak{p} \in S$ ,  $\Gamma$  is *unbounded* in  $\mathrm{GL}_{n_0}(k_{\mathfrak{p}})$ .
- (3) For any  $\mathbb{Q}$ -almost simple factor  $\mathbb{G}_1^{(i)}$  of the Zariski-closure  $\mathbb{G}_1$  of  $\Gamma$  in  $R_{k/\mathbb{Q}}(\mathbb{G})$ ,  $\mathrm{pr}_i(\mathrm{Ad}(\overline{\Omega}))$  *freely generates* a Zariski-dense subgroup of  $\mathrm{Ad}(\mathbb{G}_1^{(i)})$ .
- (4) For any proper algebraic  $\mathbb{Q}$ -subgroup  $\mathbb{H}$  of  $\mathbb{G}_1$  and positive integer  $l \gg_{\Omega} 1$ , we have

$$\mathcal{P}_{\Omega}^{(l)}(\mathbb{H}(\mathbb{Q})) \leq e^{-\Theta_{\Omega}(l)}.$$

- (5)  $\{\mathrm{Cay}(\pi_{\mathfrak{p}}(\Gamma), \pi_{\mathfrak{p}}(\Omega))\}_{\mathfrak{p} \in V_f(k) \setminus S}$  is a family of expanders.

It is worth pointing out that by Lemma 12 and a similar argument as in the proof of Lemma 14, we have.

**Lemma 20.** *For a given finite set of representations  $\rho_i : \mathbb{G}_1 \rightarrow \mathrm{GL}_{n_i}$  that are defined over a finite Galois extension  $k'$  of  $k$ , passing to a finite-index subgroup of  $\Gamma$ , if necessary, we can assume that the following holds: for  $\tilde{\mathfrak{p}} \in V_f(k')$ , if  $\rho_i(\Gamma)$  is a bounded subgroup of  $\mathrm{GL}_{n_i}(k'_{\tilde{\mathfrak{p}}})$ , then  $\rho_i(\Gamma) \subseteq \mathrm{GL}_{n_i}(\mathcal{O}_{\tilde{\mathfrak{p}}})$ .*

**2.7. Escaping from subschemes, and ramified primes of a scheme.** As it was observed in [BGS10], one of the important consequences of having spectral gap modulo primes (see Theorem 17) is the fact that the probability of hitting a proper subvariety decays exponentially (see Proposition 25). Subsets of a finitely generated group with this property are called *exponentially small* by Lubotzky-Mieri [LM13]. Since the set of non-regular elements of a semisimple group is a proper subvariety, it was observed in [LM13] that the set of non-regular elements is an exponentially small set.

Saying that  $\gamma$  is a regular element is equivalent to saying that the connected component of the centralizer subgroup  $C_{\mathbb{G}}(\gamma)$  is a (maximal) torus. In this work, however, this type of information is not enough. Here one needs to understand the structure of the centralizer subgroups  $C_{\pi_{\mathfrak{p}^n}(\Gamma)}(\pi_{\mathfrak{p}^n}(\gamma))$ . For this purpose, one needs to know that the *distance* between  $\gamma$  and the variety of non-regular elements is at least  $p^{-cn}$  for a small positive  $c$ . In fact, one needs to find such  $\gamma$  in a way that  $C_{\pi_{\mathfrak{p}^n}(\Gamma)}(\pi_{\mathfrak{p}^n}(\gamma))$  intersects a given approximate subgroup  $\pi_{\mathfrak{p}^n}(A)$  in a large set. This forces us to look at the scheme-theoretic closure of non-regular elements and its shifts by elements of  $\Gamma$ . And we have to escape these schemes in  $\Theta(n \log p)$ -steps<sup>3</sup> (see Proposition 53). Results of this section rely on the existence of points with *small* logarithmic height which is proved in Appendix A based on arithmetic Bezout.

Before stating this proposition, let us see a lemma on *ramified primes*.

**Lemma 21.** *Let  $k$  be a number field and  $S_0$  be a finite subset of  $V_f(k)$ . Let  $\mathcal{W} = \mathrm{Spec}(A)$ , where  $A = \mathcal{O}_k(S_0)[X_1, \dots, X_n]/\langle f_1, \dots, f_m \rangle$ . Suppose the generic fiber of  $\mathcal{W}$  is geometrically a complete intersection,*

<sup>3</sup>This kind of approach is inspired by [BG08-b] where they use random matrix theory to get a similar result for a Zariski-dense subgroup of  $\mathrm{SL}_n(\mathbb{Z})$ .

i.e.  $\dim(A \otimes_{\mathcal{O}_k(S_0)} \bar{k}) = n - m$ . If  $\mathfrak{p}|p$  and  $\log p \gg h := \max_i \{h(f_i)\}$  (see Appendix A for the definition of logarithmic height  $h(f)$  of a polynomial  $f$ ) where the constant depends on  $\deg f_i$ ,  $n$ , and  $k$ , then

$$\dim \mathcal{W} \times_{\mathcal{O}_k(S_0)} \bar{\mathfrak{f}}_{\mathfrak{p}} = \dim \mathcal{W} \times_{\mathcal{O}_k(S_0)} \bar{k}.$$

In particular,  $|\mathcal{W}(\mathfrak{f}_{\mathfrak{p}})| \ll p^d$ , where  $d = \dim \mathcal{W} \times_{\mathcal{O}_k(S_0)} \bar{k}$  and the implied constant depends just on  $\deg(f_i)$  and  $k$ .

*Proof.* By Lemma 67 in Appendix A, there are  $f_{k+1}, \dots, f_n \in \mathcal{O}_k(S_0)[\underline{X}]$  such that

- (1)  $\dim(k[\underline{X}]/\langle f_1, \dots, f_n \rangle) = 0$ ,
- (2)  $h(f_i) \ll h$ .

By Proposition 66 in Appendix A, Rabinowitsch trick and effective Nullstellensatz [BY91], we have that there are  $p_i(x_i) \in \mathcal{O}_k(S_0)[x_i]$  (single variable  $x_i$ ) and  $h_{ij} \in \mathcal{O}_k(S_0)[\underline{X}]$  such that

- (1) For any  $i$ ,  $p_i(x_i) = h_{i1}f_1 + \dots + h_{in}f_n$ .
- (2) For any  $i$  and  $j$ ,  $\deg p_i, \deg h_{ij} \ll 1$  and  $h(p_i), h(h_{ij}) \ll h$ , where the implied constants depend on  $\max_i \{\deg f_i\}$ ,  $n$ , and  $k$ .

Hence  $\dim(\mathcal{O}_k(S_0)[\underline{X}]/\langle f_1, \dots, f_n \rangle \otimes_{\mathcal{O}_k(S_0)} \bar{\mathfrak{f}}_{\mathfrak{p}}) = 0$  if  $\log p \gg h$ . Thus  $\dim(A \otimes_{\mathcal{O}_k(S_0)} \bar{\mathfrak{f}}_{\mathfrak{p}}) = n - m$  if  $\log p \gg h$ .

The rest can be deduced using generalized Bezout and [LW54, Lemma 1] (also see [FHJ94, Lemma 3.1]).  $\square$

**Definition 22.** Let  $k$  be a number field and  $S_0$  be a finite subset of  $V_f(k)$ . Let

$$\mathcal{W} := \text{Spec}(\mathcal{O}_k(S_0)[X_1, \dots, X_n]/\langle f_1, \dots, f_m \rangle).$$

We say  $\mathfrak{p} \in V_f(k) \setminus S_0$  is a ramified place of  $\mathcal{W}$  if  $\dim \mathcal{W} \times_{\mathcal{O}_k(S_0)} \bar{\mathfrak{f}}_{\mathfrak{p}} \neq \dim \mathcal{W} \times_{\mathcal{O}_k(S_0)} \bar{k}$ . And we let

$$p_0(\mathcal{W}) := \inf\{p \in V_f(\mathbb{Q}) \mid p' \in V_f(\mathbb{Q}), p' \geq p, \mathfrak{p}'|p' \implies \text{ is NOT a ramified place of } \mathcal{W}\}.$$

So by Lemma 21, if the generic fiber of  $\mathcal{W}$  is geometrically a complete intersection variety, then  $\log p_0(\mathcal{W}) \ll \max_i \{h(f_i)\}$ , where the implied constant depends on  $k$ ,  $n$  and  $\deg f_i$ . The next corollary shows that it is not necessary to assume that the generic fiber is geometrically a complete intersection variety.

**Corollary 23.** Let  $k$  be a number field and  $S$  be a finite subset of  $V_f(k)$ . Let

$$\mathcal{W} := \text{Spec}(\mathcal{O}_k(S)[X_1, \dots, X_n]/\langle f_1, \dots, f_m \rangle).$$

Then  $\log p_0(\mathcal{W}) \ll \max_i h(f_i)$  where the implied constant depends on  $k$ ,  $n$ , and  $\deg f_i$ .

*Proof.* Let  $d := \dim \mathcal{W} \times \bar{k}$ . By Lemma 68 in Appendix A, there are

$$\tilde{f}_1, \dots, \tilde{f}_{n-d} \in \sum_j \mathbb{Z}f_j,$$

such that  $h(\tilde{f}_i) \ll \max_j h(f_j)$  where the implied constant depends on  $n$  and  $\deg f_j$ . And the generic fiber of  $\widetilde{\mathcal{W}} := \mathcal{O}_k(S)[\underline{X}]/\langle \tilde{f}_1, \dots, \tilde{f}_{n-d} \rangle$  is geometrically a complete intersection variety. Therefore by Lemma 21 we have

$$\log p_0(\widetilde{\mathcal{W}}) \ll \max_j h(\tilde{f}_j) \ll \max_j h(f_j),$$

where the implied constants depend on  $n$  and the degree of  $f_j$ . For  $p \geq p_0(\mathcal{W})$  and  $\mathfrak{p} \in V_f(k)$  which divides  $p$  we have  $\dim \widetilde{\mathcal{W}} \times_{\mathcal{O}_k(S)} \bar{\mathfrak{f}}_{\mathfrak{p}} = d$ . On the other hand, for any  $\mathfrak{p}$  we have

$$\dim \widetilde{\mathcal{W}} \times_{\mathcal{O}_k(S)} \bar{\mathfrak{f}}_{\mathfrak{p}} \geq \dim \mathcal{W} \times_{\mathcal{O}_k(S)} \bar{\mathfrak{f}}_{\mathfrak{p}} \geq \dim \mathcal{W} \times_{\mathcal{O}_k(S)} \bar{k} = \dim \widetilde{\mathcal{W}} \times_{\mathcal{O}_k(S)} \bar{k}.$$

And so  $p_0(\widetilde{\mathcal{W}}) = p_0(\mathcal{W})$ , which implies that

$$\log p_0(\mathcal{W}) \ll \max_j h(f_j)$$

as we wished.  $\square$

**Definition 24.** Let  $\Omega$ ,  $\Gamma$ , and  $\mathbb{G}$  be as in Section 2.6. Recall that  $\mathbb{G}_1$  is the Zariski-closure of  $\Gamma$  as a subgroup  $R_{k/\mathbb{Q}}(\mathbb{G})$ . Let us denote  $p_0(\Gamma)$  be a prime such that for any prime  $p' \geq p$  we have

$$|\pi_{p'}(\Gamma)| = \Theta_{\dim \mathbb{G}_1}(p'^{\dim \mathbb{G}_1}),$$

where  $\Gamma$  is viewed as a subgroup of  $R_{\mathcal{O}_k(S_0)/\mathbb{Z}_S}(\mathrm{GL}_{n_0})(\mathbb{Z}_S)$  to define  $\pi_{p'}(\Gamma)$  (for suitable  $S$ ).

It is worth pointing out that by strong approximation  $p_0(\Gamma)$  exists.

**Proposition 25.** In the setting of Section 2.6, let  $S := \{p \in V_f(\mathbb{Q}) \mid \exists \mathfrak{p} \in S_0, \mathfrak{p} \mid p\}$ . And let  $\mathcal{G}_1$  be the Zariski-closure of  $\Gamma$  in  $R_{\mathcal{O}_k(S_0)/\mathbb{Z}_S}(\mathrm{GL}_{n_0})$ . Let  $\mathcal{W}$  be a closed  $\mathbb{Z}_S$ -subscheme of  $\mathcal{G}_1$  given by equations  $f_i$ 's. Assume that the dimension of the generic fiber of  $\mathcal{W}$  is less than  $\dim \mathbb{G}$ . Then there are a positive number  $\delta_0$  and a positive integer  $l_0$  depending on  $\mathbb{G}_1$  such that

$$\mathcal{P}_\Omega^{(l)}(\mathcal{W}(\mathbb{Z}_S)) \ll p_0(\mathcal{W})e^{-\delta_0 l},$$

where  $l \geq l_0$  and the implied constant depends on the geometric degree of the generic fiber of  $\mathcal{W}$ , and  $\Gamma$  (see Lemma 22 for the definition  $p_0(\mathcal{W})$ ).

In fact, we will see that the dependence of the implied constant on  $\Gamma$  is essentially on  $p_0(\Gamma)$ , the spectral gap of  $\mathrm{Cay}(\pi_p(\Gamma), \pi_p(\Omega))$  for  $\mathfrak{p} \in V_f(\mathbb{Q}) \setminus S$ , and  $\dim \mathbb{G}_1$ . Before proving Proposition 25, let us start with the following well-known lemma concerning the rate of convergence of a random-walk to the equidistribution.

**Lemma 26.** Let  $\bar{\Omega}$  be a symmetric generating set of a finite group  $H$ . Assume that the second largest eigenvalue of  $(*\mathcal{P}_{\bar{\Omega}})^2$  is at most  $\lambda_1^2$ , where  $*\mathcal{P}_{\bar{\Omega}} : l^2(H) \rightarrow l^2(H)$ ,  $*\mathcal{P}_{\bar{\Omega}}(f) := f * \mathcal{P}_{\bar{\Omega}}$ . Then for any  $X \subseteq H$  and any positive integer  $l$  we have

$$\left| \mathcal{P}_{\bar{\Omega}}^{(l)}(X) - \frac{|X|}{|H|} \right| \leq \lambda_1^l \sqrt{|X|}.$$

*Proof.* Let  $P : l^2(H) \rightarrow l^2(H)$  be the orthogonal projection to the constant functions, i.e.

$$P(f) := \frac{\langle f, \mathbb{1} \rangle}{\langle \mathbb{1}, \mathbb{1} \rangle} \mathbb{1},$$

where  $\mathbb{1}(h) = 1$  for any  $h \in H$  and  $\langle f_1, f_2 \rangle = \sum_{h \in H} f_1(h) \overline{f_2(h)}$ . Let  $T = *\mathcal{P}_{\bar{\Omega}}$ . Then  $T$  is a self-adjoint operator and leaves  $l^2(H)^\circ := \{f \in l^2(H) \mid \langle f, \mathbb{1} \rangle = 0\}$  invariant. Moreover, the operator norm of the restriction of  $T$  to  $l^2(H)^\circ$  is at most  $\lambda_1$ . Hence for any positive integer  $l$

$$(7) \quad \|T^l - P\| \leq \lambda_1^l.$$

On the other hand, we have that

$$(8) \quad \mathcal{P}_{\bar{\Omega}}^{(l)}(X) = \langle \chi_X, T^l(\delta_1) \rangle,$$

where  $\chi_X$  is the characteristic function of  $X$  and  $\delta_1$  is the characteristic function of  $\{1\}$ . We also notice that  $P(\delta_1) = \frac{1}{|H|} \mathbb{1}$  and so

$$(9) \quad \langle \chi_X, P(\delta_1) \rangle = \frac{|X|}{|H|}.$$

Hence by Equations (7), (8) and (9) we have

$$\left| \mathcal{P}_{\bar{\Omega}}^{(l)}(X) - \frac{|X|}{|H|} \right| = |\langle \chi_X, T^l(\delta_1) \rangle - \langle \chi_X, P(\delta_1) \rangle| = |\langle \chi_X, (T^l - P)(\delta_1) \rangle| \leq \|\chi_X\|_2 \|T^l - P\|_2 \|\delta_1\|_2 \leq \lambda_1^l \sqrt{|X|}.$$

$\square$

*Proof of Proposition 25.* For any prime  $p$  and positive integer  $l$  we have that

$$(10) \quad \mathcal{P}_\Omega^{(l)}(\mathcal{W}(\mathbb{Z}_S)) \leq \pi_p[\mathcal{P}_\Omega]^{(l)}(\mathcal{W}(\mathfrak{f}_p)).$$

On the other hand, by Theorem 17 and Lemma 26, there is  $\lambda_1 < 1$  such that for any prime  $p$  and positive integer  $l$  we have that

$$(11) \quad \left| \pi_p[\mathcal{P}_\Omega]^{(l)}(\mathcal{W}(\mathfrak{f}_p)) - \frac{|\mathcal{W}(\mathfrak{f}_p)|}{|\pi_p(\Gamma)|} \right| \leq \lambda_1^l \sqrt{|\mathcal{W}(\mathfrak{f}_p)|}.$$

So for  $p \geq p_0(\Gamma)$  (see definition 24) by Lemma 21 and Equations (10) and (11) we have that

$$(12) \quad \mathcal{P}_\Omega^{(l)}(\mathcal{W}) \ll p_0(\mathcal{W}) \left( \frac{1}{p} + \lambda_1^l p^{(d-1)/2} \right),$$

where  $d = \dim \mathbb{G}_1$ . Now it is clear that there is a positive number  $\delta_0$  depending on  $d$  and  $\lambda_1$  such that, if  $l \geq l_0(d, \lambda_1)$ , then there is a prime  $p$  with the following properties:

$$(13) \quad 1/p \leq e^{-\delta_0 l}, \quad \text{and} \quad \lambda_1^l p^{(d-1)/2} \leq e^{-\delta_0 l}.$$

Equations (12) and (13) give us that

$$\mathcal{P}_\Omega^{(l)}(\mathcal{W}) \ll p_0(\mathcal{W}) e^{-\delta_0 l},$$

where the implied constant depends on the degree of the generic fiber of  $\mathcal{W}$ ,  $d$ ,  $p_0(\Gamma)$  and  $\lambda_1$ .  $\square$

**2.8. Multiplicity bound.** In order to execute Sarnak-Xue [SX91] trick, we will be needing a lower bound on the dimension of irreducible representation of  $p$ -adic analytic groups. To that end, Howe's Kirillov theory for compact  $p$ -adic analytic groups is recalled [How77].

For any  $\mathfrak{p} \in V_f(k)$ , there is a positive integer  $a_0 := a_0(\mathfrak{p})$  such that  $\log : \mathfrak{p}^{a_0} \mathfrak{gl}_n(\mathcal{O}_{\mathfrak{p}}) \rightarrow 1 + \mathfrak{p}^{a_0} \mathfrak{gl}_n(\mathcal{O}_{\mathfrak{p}})$ , and  $\exp$  going backward, can be defined and satisfy the usual properties. It is worth mentioning that  $a_0(\mathfrak{p}) = 1$  except for finitely many  $\mathfrak{p}$ . There is a positive integer  $b_0 := b_0(\mathfrak{p})$  such that, if  $\mathfrak{h}$  is a Lie  $\mathcal{O}_{\mathfrak{p}}$ -subalgebra of  $\mathfrak{p}^{a_0} \mathfrak{gl}_n(\mathcal{O}_{\mathfrak{p}})$  and  $[\mathfrak{h}, \mathfrak{h}] \subseteq \mathfrak{p}^{b_0} \mathfrak{h}$ , then  $\exp(\mathfrak{h})$  is a subgroup of  $\mathrm{GL}_n(\mathcal{O}_{\mathfrak{p}})$ .

**Lemma 27.** *Let  $\mathfrak{h}$  be a Lie  $\mathcal{O}_{\mathfrak{p}}$ -subalgebra of  $\mathfrak{p}^{a_0} \mathfrak{gl}_n(\mathcal{O}_{\mathfrak{p}})$  and  $\mathfrak{p}^{s_0} \subseteq [\mathfrak{h}, \mathfrak{h}] \subseteq \mathfrak{p}^{b_0+1} \mathfrak{h}$  for some positive integer  $s_0$ . For any non-negative integer  $i$ , let  $H_i := \exp(\mathfrak{p}^{i-1} \mathfrak{h})$ . Let  $\rho$  be an irreducible unitary representation of  $H_1$ . Suppose*

$$m_\rho := \min\{m \in \mathbb{Z}^{\geq 0} \mid H_{m+1} \subseteq \ker \rho\}.$$

*Then  $\dim \rho \geq p^{(\lfloor (m_\rho - s_0)/v_{\mathfrak{p}}(p) \rfloor)/2}$ ,  $v_{\mathfrak{p}}$  is the  $\mathfrak{p}$ -adic valuation, i.e. power of  $\mathfrak{p}^{v_{\mathfrak{p}}(p)} \mathcal{O}_{\mathfrak{p}} = p \mathcal{O}_{\mathfrak{p}}$ .*

*Proof.* By [How77, Theorem 1.1], there is  $\psi \in \mathrm{hom}(\mathfrak{h}, S^1)$  such that

$$\mathrm{ch}(\rho)(\exp x) = |O(\psi)|^{-1/2} \sum_{\phi \in O(\psi)} \phi(x),$$

where  $\mathrm{ch}(\rho)$  is the character of  $\rho$  and  $O(\psi)$  is the coadjoint orbit of  $H_1$ . In particular,

$$(14) \quad m_\rho = m'_\psi := \min\{m \in \mathbb{Z}^{\geq 0} \mid \psi(\mathfrak{p}^{m+1} \mathfrak{h}) = 0\}.$$

We also get that  $\dim \rho = \sqrt{|O(\psi)|} = \sqrt{[H_1 : H_{1,\psi}]}$ , where  $H_{1,\psi} := \{h \in H_1 \mid \mathrm{Ad}^*(\psi) = \psi\}$ . By [How77, Lemma 1.1], we have  $H_{1,\psi} = \exp\{x \in \mathfrak{h} \mid \psi([x, \mathfrak{h}]) = 1\}$ . Hence

$$(15) \quad \dim \rho = \sqrt{[\mathfrak{h} : \mathfrak{h}(\psi)]}, \text{ where } \mathfrak{h}(\psi) := \{x \in \mathfrak{h} \mid \psi([x, \mathfrak{h}]) = 1\}.$$

**Claim:** (see [SG05, Lemma 3.3])  $\mathfrak{h}(\psi^p) = \mathfrak{h}(\psi)$  implies that  $\mathfrak{h}(\psi) = \mathfrak{h}$ .

*proof of Claim.* Let  $\kappa_\psi : \mathfrak{h} \rightarrow \mathrm{hom}(\mathfrak{h}, S^1)$ ,  $\kappa_\psi(x)(y) := \psi([x, y])$ . Then  $\kappa_\psi$  is a group homomorphism and  $\ker \kappa_\psi = \mathfrak{h}(\psi)$  is an open subgroup of  $\mathfrak{h}$ . On the other hand,  $\kappa_{\psi^p}(x) = \kappa_\psi(px)$ . Hence  $\mathfrak{h}(\psi^p) = \mathfrak{h}(\psi)$  implies that

$$\kappa_\psi(px) = 1 \implies \kappa_\psi(x) = 1.$$

Therefore  $\mathfrak{h}/\mathfrak{h}(\psi)$  is torsion-free. Since  $\mathfrak{h}(\psi)$  is an open subgroup, we conclude that  $\mathfrak{h} = \mathfrak{h}(\psi)$ .

We also notice that  $m'_{\psi p} = m'_{\psi} - v_p(p)$  if  $m'_{\psi} > v_p(p)$ . We also know that  $\mathfrak{h}(\phi) = \mathfrak{h}$  if and only if  $\phi([\mathfrak{h}, \mathfrak{h}]) = 1$ . Hence, if  $\mathfrak{h}(\phi) = \mathfrak{h}$ , then  $\mathfrak{h}(\mathfrak{p}^{s_0}\mathfrak{h}) = 1$ . Thus  $m'_{\phi} < s_0$ . Therefore we have

$$\mathfrak{h}(\psi) \subsetneq \mathfrak{h}(\psi^p) \subsetneq \cdots \subsetneq \mathfrak{h}(\psi^{p^{\lfloor (m'_{\psi} - s_0)/v_p(p) \rfloor - 1}}) \subsetneq \mathfrak{h},$$

which implies  $[\mathfrak{h} : \mathfrak{h}(\psi)] \geq p^{\lfloor (m'_{\psi} - s_0)/v_p(p) \rfloor}$ . And so  $\dim \rho \geq p^{\lfloor (m_{\rho} - s_0)/v_p(p) \rfloor/2}$ .  $\square$

**Proposition 28.** *Let  $k$  be a number field and  $S$  be a finite subset of  $V_f(k)$ . Let  $\Gamma \subseteq \mathrm{GL}_n(\mathcal{O}_k(S))$  be a finitely generated group whose Zariski-closure  $\mathbb{G}$  is a Zariski-connected semisimple group. Then for any  $\mathfrak{p} \in V_f(k) \setminus S$ ,  $n \in \mathbb{Z}^+$ , and complex irreducible representation  $\rho$  of  $\pi_{\mathfrak{p}^n}(\Gamma)$  which does not factor through  $\pi_{\mathfrak{p}^{n-1}}(\Gamma)$ , we have  $\dim \rho \geq |\pi_{\mathfrak{p}^n}(\Gamma)|^{\Theta_{\Gamma}(1)}$ .*

*Proof.* By the discussion in Section 2.4, by strong approximation, the closure  $\Gamma_{\mathfrak{p}}$  of  $\Gamma$  in  $\mathbb{G}(k_{\mathfrak{p}})$  is a  $p$ -adic analytic group. Passing to a finite-index subgroup, if needed, we can assume that either  $\Gamma_{\mathfrak{p}}$  is a hyperspecial parahoric subgroup or  $\Gamma_{\mathfrak{p}}$  is a small enough open compact subgroup that satisfies the conditions of Howe's Kirillov theory.

For any  $\mathfrak{p} \in V_f(k) \setminus S$ , let  $c_0 := 2(a_0(\mathfrak{p}) + b_0(\mathfrak{p}))$  (where  $a_0$  and  $b_0$  are described at the beginning of this section), and  $\Gamma_{\mathfrak{p}}[\mathfrak{p}^{c_0}] := \ker(\Gamma_{\mathfrak{p}} \xrightarrow{\pi_{\mathfrak{p}^{c_0}}} \pi_{\mathfrak{p}^{c_0}}(\Gamma))$ . Then  $\log$  is well-defined on  $\Gamma_{\mathfrak{p}}[\mathfrak{p}^{c_0}]$  and its image  $\mathfrak{g}_{\mathfrak{p}}$  is a Lie algebra. Moreover for some  $s_0$  (independent of  $\mathfrak{p}$ ) we have  $\mathfrak{p}^{s_0}\mathfrak{g}_{\mathfrak{p}} \subseteq [\mathfrak{g}_{\mathfrak{p}}, \mathfrak{g}_{\mathfrak{p}}]$ .

So, for  $n > c_0$ , we get the claim by Lemma 27.

For  $1 < n \leq c_0$ , we get the claim using the fact that  $\pi_{\mathfrak{p}^n}(\Gamma_{\mathfrak{p}}[\mathfrak{p}])$  is a finite  $p$ -group of order at most  $p^{\Theta_{\mathbb{G}}(1)}$ .

For  $n = 1$ ,  $\pi_{\mathfrak{p}}(\Gamma)$  is a product of almost simple finite groups of Lie type. And we get the claim using [LS74] (see [SGV12, Section 4.2]).  $\square$

**2.9. Finite logarithmic maps.** Here we recall the *finite logarithmic maps* and their main properties. These maps are the key connection between congruence groups and the Lie algebra. All of these results are well-known for Chevalley groups, but I could not find them in the literature in the generality needed for this work.

Let  $A$  be a PID and  $F$  be its field of fractions. Let  $\mathbb{H} \subseteq (\mathrm{SL}_n)_F$  be a connected  $F$ -subgroup and  $\mathcal{H}$  be its Zariski-closure in  $(\mathrm{SL}_n)_A$ ; in particular  $\mathcal{H}$  is a flat finite-type  $A$ -group scheme.

Let us recall that  $\mathrm{Lie} \mathcal{H}$  is an  $A$ -group scheme and for any  $A$ -algebra  $R$  we have that

$$(16) \quad 1 \rightarrow \mathrm{Lie} \mathcal{H}(R) \rightarrow \mathcal{H}(R[x]/\langle x^2 \rangle) \rightarrow \mathcal{H}(R) \rightarrow 1$$

is a short exact sequence. If  $\mathcal{H}$  is a *smooth*  $A$ -group scheme, then  $\mathrm{Lie} \mathcal{H} = \mathfrak{h}$ , where  $\mathfrak{h} = \mathrm{Lie} \mathcal{H}(A)$  and  $\mathfrak{h}(R) := \mathfrak{h} \otimes_A R$  for any  $A$ -algebra  $R$ . On the other hand, since the generic fiber  $\mathbb{H}$  of  $\mathcal{H}$  is smooth, there is  $a_0 \in A$  such that  $\mathcal{H} \times_A A[1/a_0]$  is a smooth  $A[1/a_0]$ -group scheme, and in particular  $\mathrm{Lie} \mathcal{H} \times_A A[1/a_0] = \mathfrak{h} \times_A A[1/a_0]$ .

To be more precise, suppose  $f_1, \dots, f_s \in A[X_{11}, \dots, X_{nn}]$  is a set of defining relations of  $\mathcal{H}$ , i.e. as an  $A$ -scheme  $\mathcal{H} = \mathrm{Spec}(A[X_{11}, \dots, X_{nn}]/\langle f_1, \dots, f_s \rangle)$ . Then as an  $A$ -scheme

$$(17) \quad \mathrm{Lie} \mathcal{H} = \mathrm{Spec}(A[X_{11}, \dots, X_{nn}]/\langle (df_1)_I, \dots, (df_s)_I \rangle),$$

where  $(df_i)_I(Y_{ij}) := \sum_{ij} (\partial f_i / \partial X_{ij})(I) Y_{ij}$ . Looking at the Taylor expansion of  $f_i$  we see that for an  $A$ -algebra  $R$  and  $Y \in M_n(R)$  we have  $(df_i)_I(Y) = 0$  if  $f_i(I + tY) = 0$  and  $t^2 = 0$  in  $R$ . Therefore, for  $q_1|q_2|q_1^2$ , we get the following maps

$$\widetilde{\Psi}_{q_1}^{q_2} : \pi_{q_2}(\mathcal{H}(A)[q_1]) \rightarrow \mathrm{Lie} \mathcal{H}(A/q_3A), \quad \widetilde{\Psi}_{q_1}^{q_2}(\pi_{q_2}(g)) := \pi_{q_3}((g-1)/q_1),$$



where  $q_3 = q_2/q_1$ ,  $\pi_q : \mathcal{H}(A) \rightarrow \mathcal{H}(A/qA)$ , and  $\mathcal{H}(A)[q] := \ker(\mathcal{H}(A) \xrightarrow{\pi_q} \mathcal{H}(A/qA))$ . Notice that  $\text{Lie } \mathcal{H}(A/q_3A)$  is *not* necessarily isomorphic to  $\mathfrak{h}/q_3\mathfrak{h}$ , but this is the case when  $q_3A$  does not have small prime factors (as it is pointed out above). In fact, by (17),  $\text{Lie } \mathcal{H}(R) = \{Y \in M_n(R) \mid F(Y) = 0\}$  where,  $F(Y) = ((df_1)_I(Y), \dots, (df_s)_I(Y))$ . So there is  $q_0 \in A$  (depending on  $f_i$ ) such that, for any  $q \in A$ ,  $\text{Lie } \mathcal{H}(A/qA)$  can be naturally mapped onto  $\mathfrak{h}/q^-\mathfrak{h}$ , where  $q^- := q/\gcd(q, q_0)$ . Hence for  $q_1|q_2|q_1^2$  we get the *finite logarithmic maps*:

$$(18) \quad \Psi_{q_1}^{q_1 q_3^-} : \pi_{q_1 q_3^-}(\mathcal{H}(A)[q_1]) \rightarrow \mathfrak{h}/q_3^-\mathfrak{h}, \quad \Psi_{q_1}^{q_1 q_3^-}(\pi_{q_1 q_3^-}(g)) := \pi_{q_3^-}(x),$$

where  $x \in \mathfrak{h} \subseteq \mathfrak{sl}_n(A)$  and  $\pi_{q_3^-}(x) = \pi_{q_3^-}((g-1)/q_1)$ .

Let  $\Gamma$  be a finitely generated subgroup of  $\text{GL}_{n_0}(\mathcal{O}_k(S))$ . Suppose the Zariski-closure  $\mathbb{G}$  of  $\Gamma$  in  $(\text{GL}_{n_0})_k$  is a connected, simply-connected semisimple group. For any  $\mathfrak{p} \in V_f(k) \setminus S$ , let  $\mathbb{G}_1$  and  $\mathbb{G}_{1,\mathfrak{p}}$  be as in Lemma 15. Hence based on the way these groups are defined we have  $\Gamma \subseteq \mathbb{G}_1(\mathbb{Q}) \cap \text{GL}_{n_0 \dim k}(\mathbb{Z}_{S_0})$ , where  $S_0 := \{p \in V_f(\mathbb{Q}) \mid \exists \mathfrak{p} \in S, \mathfrak{p}|p\}$  and  $\Gamma \subseteq \mathbb{G}_{1,\mathfrak{p}}(\mathbb{Q}_p) \cap \text{GL}_{n_0[k:k(\mathfrak{p})]}(\mathbb{Z}_p)$ . Let  $\mathcal{G}_1$  and  $\mathcal{G}_{1,\mathfrak{p}}$  be the corresponding Zariski-closures. In particular, they are flat group schemes of finite-type. Furthermore  $\mathcal{G}_1$  and  $\mathcal{G}_{1,\mathfrak{p}}$  are defined over  $\mathbb{Z}_{S_0}$  and  $\mathbb{Z}_p$ , respectively. By strong approximation, we have that the closure of  $\Gamma$  in  $\prod_{p \in V_f(\mathbb{Q}) \setminus S_0} \mathcal{G}_1(\mathbb{Z}_p)$  is an open subgroup. And for  $\mathfrak{p} \notin S$ ,  $\Gamma_{\mathfrak{p}}$  is an open subgroup of  $\mathcal{G}_{1,\mathfrak{p}}(\mathbb{Z}_p)$ . Let

$$(19) \quad \mathfrak{g}_1 := \text{Lie } \mathcal{G}(\mathbb{Z}_{S_0}), \quad \mathfrak{g}_{1,\mathfrak{p}} := \text{Lie } \mathcal{G}_{1,\mathfrak{p}}(\mathbb{Z}_p).$$

**Lemma 29.** *Let  $\Gamma$ ,  $\mathcal{G}_1$ ,  $\mathcal{G}_{1,\mathfrak{p}}$ ,  $\mathfrak{g}_1$ , and  $\mathfrak{g}_{1,\mathfrak{p}}$  be as above. Assume  $q_1|q_2|q_1^2$ ,  $q'_1|q'_2|q_1'^2$  and  $q_1|q'_1$ . Let  $q = \gcd(q_2q'_1, q_1q'_2)$ ,  $q_3 := q_2/q_1$ , and  $q'_3 := q'_2/q'_1$ . Then*

- (1) *Suppose  $q_3, q'_3$  have large prime factors (depending on  $\Gamma$ ). Let  $\Gamma[q_1] := \Gamma \cap \mathcal{G}_1(\mathbb{Z}_{S_0})[q_1]$ , and  $\mathfrak{g} := \mathfrak{g}_1$ . Then*

- (a)  $\Psi_{q_1}^{q_2} : \pi_{q_2}(\Gamma[q_1]) \rightarrow \mathfrak{g}/q_3\mathfrak{g}$  *is a well-defined, injective additive homomorphism.*  
(b)  $\Psi_{q_1}^{q_2}$  *is  $\Gamma$ -equivariant, i.e. for any  $\gamma \in \Gamma$  and  $g \in \mathcal{G}(\prod_{p \in V_f(\mathbb{Q}) \setminus S_0} \mathbb{Z}_p)$ , there is  $x \in \mathfrak{g}$  such that*  

$$\pi_{q_1 q_1^-}(g) = \pi_{q_1 q_1^-}(1 + q_1 x) \text{ and}$$

$$\Psi_{q_1}^{q_2}(\pi_{q_2}(\gamma^{-1}g\gamma)) = \pi_{q_3}(\text{Ad}(\gamma)(x)).$$

- (c) *If  $g \in \mathcal{G}_1(\mathbb{A}_{\mathbb{Q}}(S_0))[q_1]$  and  $g' \in \mathcal{G}_1(\mathbb{A}_{\mathbb{Q}}(S_0))[q'_1]$  where  $\mathbb{A}_{\mathbb{Q}}(S_0) := \prod_{p \in V_f(\mathbb{Q}) \setminus S_0} \mathbb{Z}_p$ , then  $(g, g') := g^{-1}g'^{-1}gg' \in \mathcal{G}_1(\mathbb{A}_{\mathbb{Q}}(S_0))[q_1q'_1]$ . And*

$$\Psi_{q_1 q'_1}^q(\pi_q((g, g'))) = \pi_{q/(q_1 q'_1)}([\Psi_{q_1}^{q_2}(\pi_{q_2}(g)), \Psi_{q'_1}^{q'_2}(\pi_{q'_2}(g'))]),$$

where  $[x_1, x_2] := x_1 x_2 - x_2 x_1$ .

- (2) *Suppose  $q_i$  are powers of a single prime  $p$  and  $\log_p q_1^2/q_2, \log_p q_1'^2/q'_2 \gg_{\Gamma} 1$ . Let  $\Gamma_{\mathfrak{p}}[q_1] := \Gamma_{\mathfrak{p}} \cap \mathcal{G}_{1,\mathfrak{p}}(\mathbb{Z}_p)[q_1]$ , and  $\mathfrak{g} := \mathfrak{g}_{1,\mathfrak{p}}$ . Then the same properties for  $\Psi_{q_1}^{q_2}$  hold for  $\Gamma_{\mathfrak{p}}[q_1]$  and  $\mathcal{G}_{1,\mathfrak{p}}(\mathbb{Z}_p)$  instead of  $\Gamma[q_1]$  and  $\mathcal{G}_1(\mathbb{A}_{\mathbb{Q}}(S_0))$ , respectively. Moreover  $\Psi_{q_1}^{q_2}$  is an additive group isomorphism; in fact by part (1b) it is a  $\Gamma$ -module isomorphism.*

*Proof.* Since  $\mathbb{Z}_{S_0}$  and  $\mathbb{Z}_p$  are PIDs, the above discussion shows why  $\Psi_{q_1}^{q_2}$  is well-defined. And from the definition of  $\Psi_{q_1}^{q_2}$  it is an embedding. Now one can show the rest of the claims by direct computation except the last part:  $\Psi_{q_1}^{q_2}$  is onto if  $q_i$  are powers of a single prime  $p$  and  $\log_p q_1^2/q_2, q_1'^2/q'_2 \gg_{\Gamma} 1$ .

Since  $\Gamma_{\mathfrak{p}}$  is an open subgroup of  $\mathcal{G}_{1,\mathfrak{p}}(\mathbb{Z}_p)$ , we have  $\Gamma_{\mathfrak{p}}[p^n] = \mathcal{G}_{1,\mathfrak{p}}(\mathbb{Z}_p)[p^n]$  for  $n \gg_{\Gamma} 1$ . On the other hand, the exponential map  $\exp : p^n \mathfrak{g}_{1,\mathfrak{p}}(\mathbb{Z}_p) \rightarrow \mathcal{G}_{1,\mathfrak{p}}(\mathbb{Z}_p)[p^n]$  and the logarithmic map  $\log : \mathcal{G}_{1,\mathfrak{p}}(\mathbb{Z}_p)[p^n] \rightarrow p^n \mathfrak{g}_{1,\mathfrak{p}}(\mathbb{Z}_p)$  are well-defined analytic functions and inverse of each other for  $n \gg 1$ ; in particular  $\|\exp(x) - I\|_p = \|x\|_p$  and  $\|\log g\|_p = \|g - I\|_p$ . Therefore for any  $x \in \mathfrak{g}_{1,\mathfrak{p}}(\mathbb{Z}_p)$  and large enough  $n$  (depending on  $\Gamma$ ) we have that

$$\pi_{p^{2n}}(1 + p^n x) = \pi_{p^{2n}}(\exp(p^n x)) \in \pi_{p^{2n}}(\mathcal{G}_{1,\mathfrak{p}}(\mathbb{Z}_p)[p^n]) = \pi_{p^{2n}}(\Gamma_{\mathfrak{p}}[p^n]).$$

And so  $\Psi_{q_1}^{q_2}$  is onto if  $\log_p q_1 \gg_{\Gamma} 1$ .

□

## 3. EXPANSION, APPROXIMATE SUBGROUP, AND BOUNDED GENERATION.

**3.1. Statements and notation.** In this section, three properties will be introduced, and we will explore the connections between them. The first property is about the level- $Q$  approximate subgroups, the second property is about the bounded generation of a large congruence subgroup, and the third property is about the bounded generation of a *thick top slice*.

In this section, let  $\Omega$  be a symmetric subset of  $\mathrm{GL}_{n_0}(\mathcal{O}(S))$  given as in Section 2.6. Let  $\mathcal{G}_1$  and  $\mathcal{G}_{1,\mathfrak{p}}$  be as Lemma 29. In this section,  $\pi_{p^n}$  is either the residue map from  $\mathcal{G}_1(\mathbb{Z}_p)$  to  $\mathcal{G}_1(\mathbb{Z}/p^n\mathbb{Z})$  if  $p \in V_f(\mathbb{Q}) \setminus S_0$ , or the residue map from  $\mathcal{G}_{1,\mathfrak{p}}(\mathbb{Z}_p)$  to  $\mathcal{G}_{1,\mathfrak{p}}(\mathbb{Z}/p^n\mathbb{Z})$  if  $p \in S_0$  and  $\mathfrak{p}|p$  for some  $\mathfrak{p} \in V_f(k) \setminus S$ . And accordingly we define  $\Gamma[p^n]$  to be either  $\mathcal{G}_1(\mathbb{Z}_p)[p^n] \cap \Gamma$  if  $p \in V_f(\mathbb{Q}) \setminus S_0$ , or  $\mathcal{G}_{1,\mathfrak{p}}(\mathbb{Z}_p)[p^n] \cap \Gamma$  if  $p \in S_0$  and  $\mathfrak{p}|p$  where  $\mathfrak{p} \in V_f(k) \setminus S$ .

Before formulating the precise statement, let us introduce a notation for convenience: for a finite symmetric subset  $A$  of  $\Gamma$ , a positive integer  $l$ , a prime power  $Q = p^n$ , and a positive number  $\delta$ , let  $\mathfrak{P}_Q(\delta, A, l)$  be the following statement

$$(20) \quad (\mathcal{P}_\Omega^{(l)}(A) > Q^{-\delta}) \wedge (l > \frac{1}{\delta} \log Q) \wedge (|\pi_Q(A \cdot A \cdot A)| \leq |\pi_Q(A)|^{1+\delta}).$$

**Theorem 30** (Approximate subgroups). *In the above setting, for any  $\varepsilon > 0$  there is  $\delta > 0$  such that*

$$\mathfrak{P}_Q(\delta, A, l) \text{ implies that } |\pi_Q(A)| \geq |\pi_Q(\Gamma)|^{1-\varepsilon}$$

if  $Q = p^n$  and  $Q^{\varepsilon^{\Theta_{\mathbb{G}}(1)}} \gg_\Omega 1$ .

Theorem 30 is proved using the following:

**Theorem 31** (Bounded generation). *In the above setting, for any  $0 < \varepsilon \ll_\Omega 1$ ,  $0 < \delta \ll_{\Omega, \varepsilon} 1$ , and positive integer  $C \gg_{\Omega, \varepsilon} 1$  the following holds for a finite symmetric subset  $A$  of  $\Gamma$  which contains 1:*

$$\mathcal{P}_\Omega^{(l)}(A) > Q^{-\delta} \text{ for some } l > \log Q/\delta \text{ implies that } \pi_Q(\Gamma[q]) \subseteq \prod_C \pi_Q(A) \text{ for some } q|Q \text{ such that } q < Q^\varepsilon$$

if  $Q = p^n$  and  $Q^{\varepsilon^{\Theta_{\mathbb{G}}(1)}} \gg_\Omega 1$ .

Theorem 31 is proved based on a propagation process and the following proposition.

**Proposition 32** (Thick top slice). *In the above setting, for any  $0 < \varepsilon_2 \ll_\Omega \varepsilon_1 \ll_\Omega 1$ , there are  $0 < \delta$  and a positive integer  $C = C_\Omega(\varepsilon_1, \varepsilon_2)$  with the following property:*

$$\mathfrak{P}_Q(\delta, A, l) \text{ implies that there are } X \subseteq \prod_C A \text{ and } q_1|q_2|Q \text{ such that}$$

- (1)  $q_1 \leq Q^{\varepsilon_1}$  and  $Q^{\varepsilon_2} \leq q_2/q_1$ ,
- (2)  $\pi_{q_2}(X) = \pi_{q_2}(\Gamma[q_1])$ .

if  $Q = p^n$  and  $n\varepsilon_2 \gg_\Omega 1$ .

**3.2. Theorem 30 (Approximate subgroup) implies Theorem 1 (Spectral gap).** We can assume that  $\Omega$  satisfies the extra assumptions listed in Section 2.6. By the discussion in Section 2.4, we know that  $\Gamma_{\mathfrak{p}}$  is a quotient of the closure  $\Gamma_p$  of  $\Gamma$  in  $\mathcal{G}_1(\mathbb{Z}_p)$  if  $p \in V_f(\mathbb{Q}) \setminus S_0$ . Hence  $\lambda_1(\mathcal{P}_\Omega; \Gamma_{\mathfrak{p}}) \leq \lambda_1(\mathcal{P}_\Omega; \Gamma_p)$ . For  $\mathfrak{p} \in V_f(k) \setminus S$  which divides  $p \in S_0$ , we notice that  $\Gamma_{\mathfrak{p}}[q] := \mathcal{G}_{1,\mathfrak{p}}(\mathbb{Z}_p)[q] \cap \Gamma_{\mathfrak{p}}$  is a neighborhood basis for the identity. So altogether it is enough to prove:

$$\sup\{\lambda_1(\mathcal{P}_{\pi_Q(\Omega)}; \pi_Q(\Gamma)) \mid Q = p^n; \exists \mathfrak{p} \in V_f(k) \setminus S, \mathfrak{p}|p\} < 1,$$

where  $\pi_Q$  is the residue map defined at the beginning of Section 3.1.

Let  $\mathcal{P} = \mathcal{P}_\Omega$  and let  $T_Q : l^2(\pi_Q(\Gamma)) \rightarrow l^2(\pi_Q(\Gamma))$ ,  $T_Q(f) := \pi_Q[\mathcal{P}] * f$ . Let  $\lambda_1(Q)$  be the second largest eigenvalue. We have to prove that there is a uniform upper bound for  $\lambda_1(Q)$ 's. Since  $l^2(\pi_Q(\Gamma))$  is a

completely reducible  $\pi_Q(\Gamma)$ -space, there is a unit eigenfunction  $f \in l^2(\pi_Q(\Gamma))$  such that  $T_Q(f) = \lambda_1(Q)f$  and the  $\pi_Q(\Gamma)$ -module  $V$  generated by  $f$  is irreducible. Changing  $Q$  to one of its divisors, if necessary, we can and will assume that the action of  $\pi_Q(\Gamma)$  on  $V$  does not factor through  $\pi_q(\Gamma)$  for any proper divisor  $q$  of  $Q$ . Now by Proposition 28 there is  $\varepsilon_0 > 0$  such that  $\dim V \geq |\pi_Q(\Gamma)|^{\varepsilon_0}$ . So the multiplicity of  $\lambda_1(Q)$  is at least  $|\pi_Q(\Gamma)|^{\varepsilon_0}$ . Hence

$$(21) \quad |\pi_Q(\Gamma)|^{\varepsilon_0} \lambda_1(Q)^{2l} \leq \text{Tr}(T_Q^{2l}) = |\pi_Q(\Gamma)| \|\pi_Q(\mathcal{P}^{(l)})\|_2^2$$

So it is enough to prove that  $\|\pi_Q(\mathcal{P}^{(l)})\|_2 \leq |\pi_Q(\Gamma)|^{-\frac{1}{2} + \frac{\varepsilon_0}{4}}$  for some  $l \ll \log Q$  where the implied constant just depends on  $\Omega$ .

**Lemma 33.** *Let  $\Omega$  and  $\varepsilon_0$  be as above. Then there is  $\delta > 0$  with the following property:*

*let  $Q = p^n$ , where some  $\mathfrak{p} \in V_f(k) \setminus S$  divides  $p$ , and  $l_0 \gg \log Q$ .*

- (1)  $\|\pi_Q[\mathcal{P}^{(l_0)}]\|_2 \leq |\pi_Q(\Gamma)|^{-\delta}$ ,
- (2) *If  $l \geq \frac{1}{\delta} \log Q$  and  $\|\pi_Q[\mathcal{P}^{(l)}]\|_2 \geq |\pi_Q(\Gamma)|^{-\frac{1}{2} + \frac{\varepsilon_0}{4}}$ , then  $\|\pi_Q[\mathcal{P}^{(2l)}]\|_2 \leq \|\pi_Q[\mathcal{P}^{(l)}]\|_2^{1+\delta}$ .*

Repeated use of Lemma 33, in finitely many steps (the number of steps is independent of  $Q$ ), would give us  $l \ll \log Q$  such that  $\|\pi_Q[\mathcal{P}^{(l)}]\|_2 \leq |\pi_Q(\Gamma)|^{-\frac{1}{2} + \frac{\varepsilon_0}{4}}$  as we desired. So in order to complete this step, it is enough to prove Lemma 33.

*Proof of Lemma 33.* First we notice that by Kesten's bound, there is  $l_0 \gg \log Q$  and  $\delta_1 > 0$  such that  $\|\pi_Q[\mathcal{P}^{(l)}]\|_2 \leq |\pi_Q(\Gamma)|^{-\delta_1}$  for  $l \geq l_0$ .

Now to get the second part, we proceed by contradiction. So assume for small enough  $\delta > 0$  (specified later), we have  $\|\mu\|_2^2 \geq |\pi_{Q_\delta}(\Gamma)|^{-1+\varepsilon_0/2}$  and  $\|\mu * \mu\|_2 \geq \|\mu\|_2^{1+\delta}$ , where  $\mu = \pi_{Q_\delta}[\mathcal{P}^{(l_\delta)}]$  for some  $l_\delta \geq \frac{1}{\delta} \log Q_\delta$ . Thus by Lemma 7 there is a subset  $\overline{A}_\delta$  of  $\pi_{Q_\delta}(\Gamma)$  with the following properties:

- (1)  $\|\mu\|_2^{-2+R\delta} \leq |\overline{A}_\delta| \leq \|\mu\|_2^{-2-R\delta}$ ,
- (2)  $|\prod_3 \overline{A}_\delta| \leq |\overline{A}_\delta| \cdot \|\mu\|_2^{-R\delta}$ ,
- (3) For any  $\overline{h} \in \overline{A}_\delta$ ,  $(\mu * \mu)(\overline{h}) \geq \frac{\|\mu\|_2^{R\delta}}{|\overline{A}_\delta|}$ .

These conditions imply that there is  $\delta' := \delta'(\delta)$  with the following properties:

- (1)  $\lim_{\delta \rightarrow 0+} \delta' = 0$  and  $\delta'(\delta) \geq \delta$ ,
- (2)  $|\prod_3 \overline{A}_\delta| \leq |\overline{A}_\delta|^{1+\delta'}$ ,
- (3)  $\mu^{(2)}(\overline{A}_\delta) \geq Q_\delta^{-\delta'}$ .

Now let  $A_\delta = \pi_{Q_\delta}^{-1}(\overline{A}_\delta) \cap \text{supp}(\mathcal{P}^{(2l_\delta)})$ . By the definition,  $\mathcal{P}^{(2l_\delta)}(A_\delta) = \pi_{Q_\delta}[\mathcal{P}^{(2l_\delta)}](\overline{A}_\delta)$  and  $\pi_{Q_\delta}(A_\delta) = \overline{A}_\delta$  (equality holds as  $\pi_Q[\mathcal{P}^{(2l_\delta)}](\overline{h}) > 0$  for any  $\overline{h} \in \overline{A}_\delta$ ); moreover since  $\mathcal{P}$  and  $\overline{A}_\delta$  are symmetric,  $A$  is also symmetric. Hence for  $0 < \delta \ll 1$ , we end up with a symmetric finite subset  $A_\delta$  of  $\Gamma$  with the following properties:

- (1)  $\mathcal{P}^{(2l_\delta)}(A_\delta) \geq Q_\delta^{-\delta'}$  and  $2l_\delta > \frac{1}{\delta'} \log Q_\delta$ ,
- (2)  $|\pi_{Q_\delta}(A_\delta \cdot A_\delta \cdot A_\delta)| \leq |\pi_{Q_\delta}(A_\delta)|^{1+\delta'}$ ,
- (3)  $|\pi_{Q_\delta}(A_\delta)| \leq |\pi_{Q_\delta}(\Gamma)|^{1-\varepsilon_0/4}$ .

Since  $l_\delta > \log Q_\delta/\delta$ , we have  $\lim_{\delta \rightarrow 0} l_\delta = \infty$ . Now we claim that  $Q_\delta \rightarrow \infty$  as  $\delta \rightarrow 0$ . If not, for infinitely many  $\delta$  we have  $Q_\delta = Q$ , and  $\pi_Q(A_\delta) = \overline{A}$  is independent of  $\delta$ . And so

$$\lim_{\delta \rightarrow 0} \pi_Q[\mathcal{P}^{(l_\delta)}](\pi_Q(A_\delta)) = \frac{|\overline{A}|}{|\pi_Q(\Gamma)|} < \frac{1}{|\pi_Q(\Gamma)|^{\varepsilon_0}}.$$

On the other hand, we have

$$\pi_Q[\mathcal{P}]^{(l_\delta)}(\pi_Q(A_\delta)) \geq \mathcal{P}^{(l_\delta)}(A_\delta) > Q_\delta^{-\delta} = Q^{-\delta}.$$

Hence as  $\delta \rightarrow 0$ , we get  $|\pi_Q(\Gamma)|^{-\varepsilon_0} > 1$ , which is a contradiction. Since  $Q_\delta$  gets arbitrarily large, Theorem 30 gives us the desired contradiction.  $\square$

**3.3. Theorem 31 (Bounded generation) implies Theorem 30 (Approximate subgroup).** By the contrary assumption, there is  $\varepsilon_0 > 0$  such that for any  $\delta > 0$  there are a finite symmetric subset  $A_\delta$ , a positive integer  $l_\delta$  and  $Q_\delta \in \{p^n \mid \exists \mathfrak{p} \in V_f(k) \setminus S, \mathfrak{p} \nmid p\}$  such that  $\mathfrak{P}_{Q_\delta}(\delta, A_\delta, l_\delta)$  holds and at the same time  $|\pi_{Q_\delta}(A_\delta)| < |\pi_{Q_\delta}(\Gamma)|^{1-\varepsilon_0}$ .

By a similar argument as in the end of Section 3.2, we have  $Q_\delta \rightarrow \infty$  as  $\delta \rightarrow 0$ .

By Theorem 31, for any  $0 < \varepsilon' \ll 1$  there is  $C = C_\Omega(\varepsilon')$  such that for any  $0 < \delta \ll_{\varepsilon', \Omega} 1$

$$(22) \quad \pi_{Q_\delta}(\Gamma[q_\delta]) \subseteq \prod_C \pi_{Q_\delta}(A_\delta),$$

for some  $q_\delta | Q_\delta$  such that  $q_\delta < Q_\delta^{\varepsilon'}$ . Hence

$$(23) \quad |\pi_{Q_\delta}(\prod_C A_\delta)| \geq |\pi_{Q_\delta}(\Gamma)|^{1-\Theta_\Omega(\varepsilon')},$$

for small enough  $\delta$  (depending on  $\varepsilon'$ ) as  $\lim_{\delta \rightarrow 0} Q_\delta = \infty$ . On the other hand, since  $|\pi_{Q_\delta}(\prod_C A_\delta)| \leq |\pi_{Q_\delta}(A_\delta)|^{1+\delta}$  by the Ruzsa inequality (see [Hel05]), we have

$$(24) \quad |\pi_{Q_\delta}(\prod_C A_\delta)| \leq |\pi_{Q_\delta}(A_\delta)|^{1+(C-2)\delta} \leq |\pi_{Q_\delta}(\Gamma)|^{(1-\varepsilon_0)(1+(C-2)\delta)}.$$

By (23) and (24), for any  $\varepsilon'$  and small enough  $\delta$  (in particular it can approach zero), we have

$$1 - \Theta_\Omega(\varepsilon') \leq (1 - \varepsilon_0)(1 + (C(\varepsilon') - 2)\delta),$$

which is a contradiction.

**3.4. Proposition 32 (Thick top slice) implies Theorem 31 (Bounded generation).** First we discuss that changing  $A$  to  $\prod_{O_\Omega(1)} A$ , if needed, we can and will assume  $\mathfrak{P}(\delta, A, l)$  holds. Next we deal with a given large  $N$ . Then we finish the proof using Proposition 32 and a propagation process based on taking commutators (a similar approach is used in [BG08-b, BG09]).

**Lemma 34.** *Let  $\Omega$  and  $Q$  be as in Proposition 31. For any  $0 < \delta_0 \ll_\Omega 1$  and a finite symmetric subset  $A$  of  $\Gamma$  which contains 1 the following holds*

$$\mathcal{P}^{(l)}(A) > Q^{-\delta_0} \text{ for some positive integer } l > \log Q/\delta_0 \text{ implies } \mathfrak{P}(\delta_0, \prod_{O_\Omega(1)} A, l) \text{ holds.}$$

*Proof.* For small enough  $c := c(\Omega)$ ,  $\pi_Q$  induces an injection from  $B_{\lceil c \log Q \rceil}$  into  $\pi_Q(\Gamma)$ . In particular,  $|\pi_Q(A \cdot A)| \geq |A \cdot A \cap B_{\lceil c \log Q \rceil}|$ . By Lemma 6, we have  $\mathcal{P}^{(\lceil c \log Q \rceil)}(A \cdot A) \geq Q^{-2\delta_0}$  as  $\lceil c \log Q \rceil/2 < \log Q/\delta_0 < l$ . Hence by Kesten's bound we have

$$Q^{-2\delta_0} \leq \mathcal{P}^{(\lceil c \log Q \rceil)}(A \cdot A) \leq |A \cdot A \cap B_{\lceil c \log Q \rceil}| Q^{-\Theta_\Omega(1)}.$$

Therefore  $|\pi_Q(A \cdot A)| \geq Q^{\Theta_\Omega(1)-2\delta_0} = Q^{\Theta_\Omega(1)}$  for  $0 < \delta_0 \ll_\Omega 1$ . Hence for some  $C' := C'(\Omega)$  we have  $|\pi_Q(\prod_{C'} A) \cdot \pi_Q(\prod_{C'} A)| \leq \pi_Q(\prod_{C'} A)^{1+\delta_0}$ . Since  $1 \in A$ ,  $\prod_{C'} A \supseteq A$ . And so  $\mathcal{P}^{(l)}(\prod_{C'} A) \geq \mathcal{P}^{(l)}(A) > Q^{-\delta_0}$ , which implies that  $\mathfrak{P}(\delta_0, \prod_{C'} A, l)$  holds.  $\square$

**Lemma 35.** *Let  $\Omega$  be as in Section 2.6. Then for any positive integer  $N$  there are  $\delta > 0$  and a positive integer  $C$  which depends on  $\Omega$  and  $N$  such that*

$$\mathfrak{P}_Q(\delta, A, l) \text{ implies that } \pi_Q(\Gamma) = \prod_C \pi_Q(A)$$

if  $Q = p^N$  and  $p \gg_\Omega 1$ .

*Proof.* Let  $\mathcal{G}_1$  be as in Lemma 29. Based on the discussion in Section 2.4, for  $p \gg_\Omega 1$ , we have that  $\Gamma$  is dense in  $\mathcal{G}_1(\mathbb{Z}_p)$ . By Theorem 17, Lemma 26, and  $l > \frac{N}{\delta} \log p$ , we have that

$$\left| \pi_p[\mathcal{P}]^{(l)}(\pi_p(A)) - \frac{|\pi_p(A)|}{|\pi_p(\Gamma)|} \right| \leq \frac{1}{|\pi_p(\Gamma)|}$$

for small enough  $\delta$ . And so we have

$$p^{-N\delta} = Q^{-\delta} \leq \pi_p[\mathcal{P}]^{(l)}(\pi_p(A)) \leq \frac{|\pi_p(A)| + 1}{|\pi_p(\Gamma)|},$$

which implies that  $|\pi_p(A)| \geq |\pi_p(\Gamma)|^{1-\Theta_{\Omega,N}(\delta)}$ . On the other hand, for  $p \gg_\Omega 1$ ,  $\pi_p(\Gamma) = \mathcal{G}_1(\mathbb{Z}/p\mathbb{Z})$  is a product of almost simple groups and so it is a quasi-random group (see [SGV12, Corollary 14] and [LS74]). Hence by a result of Gowers [Gow08] (see [NP11]), for small enough  $\delta$ , we have

$$(25) \quad \pi_p(A \cdot A \cdot A) = \pi_p(\Gamma).$$

If  $p$  is large enough,  $\Gamma$  is dense in  $\mathcal{G}_1(\mathbb{Z}_p)$ ,  $\mathcal{G}_1(\mathbb{Z}_p)$  is a hyper-special parahoric subgroup,

$$(26) \quad 1 \rightarrow \text{Lie}(\mathcal{G}_1)(\mathbb{Z}/p\mathbb{Z}) \rightarrow \mathcal{G}_1(\mathbb{Z}/p^2\mathbb{Z}) \xrightarrow{\pi_p} \mathcal{G}_1(\mathbb{Z}/p\mathbb{Z}) \rightarrow 1$$

is a short exact sequence, and  $\text{Lie}(\mathcal{G}_1)(\mathbb{Z}/p\mathbb{Z}) = \underline{\mathfrak{g}}_1(\mathbb{Z}/p\mathbb{Z})$ . Moreover  $\underline{\mathfrak{g}}_1(\mathbb{Z}/p\mathbb{Z}) = \bigoplus_j \mathfrak{g}_j$  where  $\mathfrak{g}_j$ 's are simple Lie algebras and simple  $\mathcal{G}_1(\mathbb{Z}/p\mathbb{Z})$ -modules under the adjoint representation.

By (25), there is a section  $\psi : \mathcal{G}_1(\mathbb{Z}/p\mathbb{Z}) \rightarrow \prod_3 A \subseteq \Gamma$  of  $\pi_p : \Gamma \rightarrow \mathcal{G}_1(\mathbb{Z}/p\mathbb{Z})$ . Let  $\psi_p := \pi_{p^2} \circ \psi : \mathcal{G}_1(\mathbb{Z}/p\mathbb{Z}) \rightarrow \mathcal{G}_1(\mathbb{Z}/p^2\mathbb{Z})$ .

**Claim.** For any  $j$ , projection of  $\text{Im}(\psi_p) \cdot \text{Im}(\psi_p) \cdot \text{Im}(\psi_p)^{-1} \cap \underline{\mathfrak{g}}_1(\mathbb{Z}/p\mathbb{Z})$  to  $\mathfrak{g}_j$  is non-trivial.

*Proof of Claim.* For any  $x, y \in \mathcal{G}_1(\mathbb{Z}/p\mathbb{Z})$ ,  $\psi_p(x)\psi_p(y)\psi_p(xy)^{-1} \in \ker \pi_p = \bigoplus_j \mathfrak{g}_j$ . Now suppose to the contrary that the projection of  $\text{Im}(\psi_p) \cdot \text{Im}(\psi_p) \cdot \text{Im}(\psi_p)^{-1} \cap \underline{\mathfrak{g}}_1(\mathbb{Z}/p\mathbb{Z})$  to  $\mathfrak{g}_{j_0}$  is zero. Let's consider

$$\phi_p : \mathcal{G}_1(\mathbb{Z}/p\mathbb{Z}) \rightarrow \mathcal{G}_1(\mathbb{Z}/p^2\mathbb{Z})/(\bigoplus_{j \neq j_0} \mathfrak{g}_j), \phi_p(x) := \psi_p(x)(\bigoplus_{j \neq j_0} \mathfrak{g}_j).$$

By the contrary assumption,  $\phi_p$  is a group homomorphism. And so it is a group embedding. On the other hand, by [Wei84, Theorem 7.2],  $\langle \text{Im}(\psi_p) \rangle = \pi_{p^2}(\langle \text{Im}(\psi) \rangle) = \mathcal{G}_1(\mathbb{Z}/p^2\mathbb{Z})$  if  $p$  is large enough. Since  $\phi_p$  is a group homomorphism,  $\text{Im}(\phi_p) = \text{Pr}(\langle \text{Im}(\psi_p) \rangle)$ , where  $\text{Pr} : \mathcal{G}_1(\mathbb{Z}/p^2\mathbb{Z}) \rightarrow \mathcal{G}_1(\mathbb{Z}/p^2\mathbb{Z})/(\bigoplus_{j \neq j_0} \mathfrak{g}_j)$ . Therefore  $\phi_p$  is onto, which contradicts the fact that  $|\mathcal{G}_1(\mathbb{Z}/p\mathbb{Z})| < |\mathcal{G}_1(\mathbb{Z}/p^2\mathbb{Z})/(\bigoplus_{j \neq j_0} \mathfrak{g}_j)|$ .

The above claim implies that  $\pi_{p^2}(\prod_9 A) \cap \underline{\mathfrak{g}}_1(\mathbb{Z}/p\mathbb{Z})$  generates  $\underline{\mathfrak{g}}_1(\mathbb{Z}/p\mathbb{Z})$  as a  $\mathcal{G}_1(\mathbb{Z}/p\mathbb{Z})$ -module. Hence by [SGV12, Corollary 31] we have that

$$(27) \quad \pi_{p^2}(\prod_{O_{\dim \mathbb{G}}(1)} A) = \pi_{p^2}(\Gamma),$$

where  $\mathbb{G}$  is the generic fiber of  $\mathcal{G}_1$ .

For large enough  $p$  and any positive integer  $i$ ,  $\mathcal{G}_1(\mathbb{Z}_p)[p^i]/\mathcal{G}_1(\mathbb{Z}_p)[p^{i+1}] \simeq \underline{\mathfrak{g}}_1(\mathbb{Z}/p\mathbb{Z})$  and  $[\underline{\mathfrak{g}}_1(\mathbb{Z}/p\mathbb{Z}), \underline{\mathfrak{g}}_1(\mathbb{Z}/p\mathbb{Z})] = \underline{\mathfrak{g}}_1(\mathbb{Z}/p\mathbb{Z})$ . Hence by Lemma 29 and Equation (27), we get the desired result.  $\square$

To understand the propagation process, the following definition is helpful.

**Definition 36.** Let  $\Omega$ ,  $A$  and  $\varepsilon$  be as above. For positive real numbers  $L$  (level) and  $T$  (thickness), we say that  $\mathcal{B}(L, T) := \mathcal{B}_{Q, \varepsilon}(L, T)$  (bounded generation at the level  $L$  and of thickness  $T$ ) holds if for some divisors  $q$  and  $q'$  of  $Q$  we have  $q \leq L$ ,  $LT \leq qq'$  and

$$\pi_{qq'}(\Gamma[q]) \subseteq \pi_{qq'}(\prod_{O(1)} A),$$

where the implied constant depends only on  $\Omega$  and  $\varepsilon$ .

We present a propagation process which implies that if  $\mathcal{B}(Q^{\varepsilon_1}, Q^{\varepsilon_2})$  holds, then  $\mathcal{B}(Q^{c\varepsilon_1}, Q^{1-c\varepsilon_1})$  holds for a constant  $c$  which depends on  $\varepsilon_1/\varepsilon_2$ . To get such a process, we prove the following lemma.

**Lemma 37.** *There is a constant  $q_0$  which depends on  $\Omega$  with the following property: if  $\mathcal{B}(L, T)$  and  $\mathcal{B}(L', q_0 p)$  hold,  $L, L' \geq T$  and  $\log_p T \gg_\Omega 1$ , then  $\mathcal{B}(q_0 LL', T/q_0)$  holds.*

**Corollary 38.** *Let  $c$  be a fixed positive number, and  $q_0$  as in Lemma 37. Then, if  $L, L' \geq T \geq Q^{c\varepsilon}$ ,  $c\varepsilon \log_p Q \gg_\Omega 1$ , and  $\mathcal{B}(L, T)$  and  $\mathcal{B}(L', T')$  hold, then  $\mathcal{B}(q_0 LL', TT'/pq_0^2)$  holds.*

*Proof.* Since  $\mathcal{B}(L', T')$  holds,  $\mathcal{B}(L'(T/(q_0 p))^i, q_0 p)$  holds for any  $0 \leq i < \lfloor \log T' / \log(T/q_0 p) \rfloor < 1/(c\varepsilon)$ . Using Lemma 37 for  $\mathcal{B}(L, T)$  and  $\mathcal{B}(L'(T/(q_0 p))^i, q_0 p)$ , we conclude that  $\mathcal{B}(q_0 LL'(T/(q_0 p))^i, T/q_0)$  holds for any  $0 \leq i < 1/(c\varepsilon)$ . This implies that  $\mathcal{B}(q_0 LL', TT'/pq_0^2)$  holds.  $\square$

**Corollary 39.** *Let  $c$  be a fixed positive number, and  $q_0$  as in Lemma 37. Then, if  $L'/q_0 p \geq L \geq Q^{c\varepsilon}$ ,  $c\varepsilon \log_p Q \gg_\Omega 1$ , and  $T \geq q_0^2 p$  and  $\mathcal{B}(L, T)$  and  $\mathcal{B}(L', q_0 L)$  hold, then  $\mathcal{B}(L', Q/L')$  holds.*

*Proof.* By induction on  $i$  and Corollary 38 we can show that  $\mathcal{B}((q_0 L)^i L', q_0 L)$  for any  $i \ll_{\Omega, \varepsilon} 1$ . This easily implies the claim.  $\square$

Now we have enough to prove Proposition 32.

*Proof of Theorem 31.* Let  $c_1$  and  $c_2$  be two positive constants such that for any  $0 < \varepsilon < 1$ ,  $\varepsilon_1 := c_1 \varepsilon$  and  $c_2 \varepsilon_2$  satisfy the required inequalities of Proposition 32.

By assumption,  $Q^{\varepsilon^{(1)}} \gg_\Omega 1$ . So we can assume that  $n\varepsilon^2 \log p \gg_\Omega 1$ . Let's assume that  $\varepsilon \leq c_2^2$ . Hence  $(c_2 \varepsilon n)(c_2 \log p) \gg_\Omega 1$ . Now we choose  $c_2$  small enough so that, if  $c_2 \varepsilon n$  is not large enough for us to be able to use either Proposition 32, Corollary 38, or Corollary 39, then  $p$  is large enough that we can use Lemma 35. In the latter case, we are done. So we can and will assume that  $c_2 \varepsilon n$  is large enough (depending on  $\Omega$ ) that we can apply Proposition 32, Corollary 38, or Corollary 39. In particular, there are  $0 < \delta, C := C(c_1 \varepsilon, c_2 \varepsilon)$ , and  $q_1, q_2 | Q$  such that

- (1)  $q_1 \leq Q^{\varepsilon_1}$  and  $Q^{\varepsilon_2} \leq q_2/q_1$ ,
- (2)  $\pi_{q_2}(\Gamma[q_1]) \subseteq \pi_{q_2}(\prod_C A)$ .

We also notice that we can assume  $q_1 | q_2 | q_1^2$  (by increasing  $q_1$  or decreasing  $q_2$  if necessary). So we can assume that  $\mathcal{B}(Q^{c_1 \varepsilon}, Q^{c_2 \varepsilon})$  holds. Let  $a_0 := nc_1 \varepsilon$ ,  $b_0 := nc_2 \varepsilon$ , and  $d_0 := v_p(q_0) + 1$ , where  $q_0$  is the constant given in Lemma 37. So applying Corollary 38 repeatedly, we get that  $\mathcal{B}(p^{a_m}, p^{b_m})$  holds where

$$a_m := 2a_{m-1} + d_0, \quad b_m := 2b_{m-1} - d_0,$$

for  $m \leq \log_2 \lceil c_1/c_2 \rceil$ . Notice that  $a_m = (a_0 + d_0)2^m - d_0$  and  $b_m = (b_0 - d_0)2^m + d_0$ . In particular, for  $m_0 := \log_2 \lceil c_1/c_2 \rceil$ , we have  $b_{m_0} > a_0$ . Hence  $\mathcal{B}(Q^{c\varepsilon}, Q^{c_1 \varepsilon})$  holds for some constant  $c = c(c_1, c_2)$ . Thus, by Corollary 39,  $\mathcal{B}(Q^{c\varepsilon}, Q^{1-c\varepsilon})$  holds as  $\mathcal{B}(Q^{c_1 \varepsilon}, Q^{c_2 \varepsilon})$  and  $\mathcal{B}(Q^{c\varepsilon}, Q^{c_1 \varepsilon})$  hold.  $\square$

So it is enough to prove Lemma 37. As in the previous related works (see [BG08-b, BG09, BV12, Din06, GS04]), we use the connection between congruence subgroups and the Lie algebra.

*Proof of Lemma 37.* Finite logarithmic maps are key in this proof (see Lemma 29). The definition of these maps rely on fixing an embedding of  $\Gamma$  into either  $\mathrm{GL}_{n_0 \dim k}(\mathbb{Z}_{S_0})$  or  $\mathrm{GL}_{n_0 \dim k(\mathfrak{p})}(\mathbb{Z}_p)$ . Now let  $\mathcal{G}_1$  and  $\mathcal{G}_{1,p}$  be as in Lemma 29, and  $\mathfrak{g}_1 := \mathrm{Lie}(\mathcal{G}_1)(\mathbb{Z}_{S_0})$  and  $\mathfrak{g}_{1,p} := \mathrm{Lie}(\mathcal{G}_{1,p})(\mathbb{Z}_p)$ .

Since we treat all the primes at the same time, let

$$\mathfrak{g} := \begin{cases} \mathfrak{g}_1(\mathbb{Z}_p) & \text{if } p \in V_f(\mathbb{Q}) \setminus S_0, \\ \mathfrak{g}_{1,p}(\mathbb{Z}_p) & \text{if } \exists \mathfrak{p} \in V_f(k) \setminus S, \mathfrak{p} | p. \end{cases}$$

We also note that  $\mathfrak{g} \subseteq \mathfrak{g}_n(\mathbb{Z}_p)$  where  $n$  is either  $n_0 \dim k$  or  $n_0 \dim k(\mathfrak{p})$ . Since  $\mathbb{Z}_{S_0}$  and  $\mathbb{Z}_p$  are PID, there are positive integers  $m_1, \dots, m_d$  with the following properties: for any prime  $p$  which is divisible by some

$\mathfrak{p} \in V_f(k) \setminus S$  we have that  $\mathfrak{gl}_n(\mathbb{Z}_p)$  has a  $\mathbb{Z}_p$ -basis  $\{\tilde{x}_1, \dots, \tilde{x}_{n^2}\}$  such that  $\{x_i = m_{j_i} \tilde{x}_i\}_{i=1}^{\text{rank}_{\mathbb{Z}_p} \mathfrak{g}}$  forms a  $\mathbb{Z}_p$ -basis of  $\mathfrak{g}$ .

Since  $\mathfrak{g}$  is perfect and  $\mathfrak{g}_1$  is a  $\mathbb{Z}_{S_0}$ -Lie algebra, there is a positive integer  $q_0$  such that  $q_0 \mathfrak{g} \subseteq [\mathfrak{g}, \mathfrak{g}]$ . We also assume that  $q_0$  is a common multiple of  $m_i$ 's.

We claim that  $q_0$  has the desired property. By strong approximation, we can choose the implied constant in  $\log_p L' \geq \log_p T \gg 1$  large enough so that, for some  $q' \leq L'$ ,  $\Psi_{q'}^{q'q_0p}$  is an isomorphism. Since  $\mathcal{B}(L', q_0p)$  holds, there are  $\gamma_i \in \prod_{O_{\Omega, \varepsilon}(1)} A$  such that  $\Psi_{q'}^{q'q_0p}(\pi_{q'q_0p}(\gamma_i)) = \pi_{q_0p}(x_i)$  for any  $i$ . On the other hand, since  $\mathcal{B}(L, T)$  holds, there are  $q_1 \leq L$ ,  $q_2 \geq LT$  and a subset  $Y$  of  $\prod_{O_{\Omega, \varepsilon}(1)} A$  such that  $\Psi_{q_1}^{q_2}(\pi_{q_2}(Y)) = \pi_{q_3}(\mathfrak{g})$ , where  $q_3 = q_2/q_1$  (since  $\log_p T \gg_{\Omega} 1$ , we can talk about  $\Psi_{q_1}^{q_2}(\pi_{q_2}())$ ). Thus by Lemma 29, parts (2-a) and (2-c), we have that

$$\begin{aligned} \Psi_{q_1q'}^{q_2q'}(\pi_{q_2q'}((\prod_{O_{\Omega, \varepsilon}(1)} A) \cap \Gamma[q_1q'])) &\supseteq \sum_i \Psi_{q_1q'}^{q_2q'}(\pi_{q_2q'}((\gamma_i, Y))) \\ &\supseteq \sum_i [\Psi_{q'}^{q'q_3}(\pi_{q'q_3}(\gamma_i)), \Psi_{q_1}^{q_2}(\pi_{q_2}(Y))]. \end{aligned}$$

So there are  $y_i$ 's in  $\mathfrak{g}$  such that  $\pi_{q_0p}(y_i) = \pi_{q_0p}(x_i)$  for any  $i$  and

$$(28) \quad \pi_{q_3}(\sum_i \text{ad}(y_i)(\mathfrak{g})) \subseteq \Psi_{q_1q'}^{q_2q'}(\pi_{q_2q'}((\prod_{O_{\Omega, \varepsilon}(1)} A) \cap \Gamma[q_1q'])).$$

Since  $y_i \in \mathfrak{g}$ , there are  $m_{ij} \in \mathbb{Z}_p$  such that  $y_i = \sum_{j=1}^{\text{rank}_{\mathbb{Z}_p} \mathfrak{g}} m_{ij} x_j = \sum_{j=1}^{\text{rank}_{\mathbb{Z}_p} \mathfrak{g}} m_{ij} m_j \tilde{x}_j$ . Now as  $\pi_{q_0p}(y_i) = \pi_{q_0p}(x_i)$ , we have that  $m_{ij} m_j = \delta_{ij} m_j \pmod{q_0p}$  for any  $i$  and  $j$ , where  $\delta_{ij}$  is one if  $i = j$  and zero otherwise. Therefore  $[m_{ij}] = I \pmod{p}$  which implies that  $[m_{ij}] \in \text{GL}_d(\mathbb{Z}_p)$  and so  $\pi_{q_3}(\sum_i \mathbb{Z}_p y_i) = \pi_{q_3}(\mathfrak{g})$ . Hence by Equation (28) we have that  $q_0 \pi_{q_3}(\mathfrak{g}) \subseteq \pi_{q_3}([\mathfrak{g}, \mathfrak{g}]) \subseteq \Psi_{q_1q'}^{q_2q'}(\pi_{q_2q'}((\prod_{O_{\Omega, \varepsilon}(1)} A) \cap \Gamma[q_1q'])))$ . This means that

$$\pi_{q_3/p^{v_p(q_0)}}(\mathfrak{g}) \subseteq \Psi_{q_1q'p^{v_p(q_0)}}^{q_2q'}(\pi_{q_2q'}((\prod_{O_{\Omega, \varepsilon}(1)} A) \cap \Gamma[q_1q'p^{v_p(q_0)}])),$$

which implies that  $\mathcal{B}(LL'q_0, T/q_0)$  holds.  $\square$

#### 4. PROOF OF PROPOSITION 32 (THICK TOP SLICE).

**4.1. Finding a basis consisting of vectors with small height.** In this section, we prove the following proposition.

**Proposition 40.** *Let  $\Omega$  and  $\Gamma$  be as in Section 2.6. Let  $\mathbb{G}_1$  be as in Section 2.4. Let  $k'$  be a number field, and  $S' \subseteq V_f(l)$  be a finite subset. Let  $\rho : \mathbb{G}_1 \rightarrow \text{GL}(\mathbb{V})$  be an  $k'$ -representation such that  $\rho(\Gamma) \subseteq \text{GL}_d(\mathcal{O}_{k'}(S'))$ .*

*Then for any  $0 < \delta \ll_{\rho, \Omega} \varepsilon \ll_{\rho, \Omega} 1$  the following holds:*

*If  $Q$  is a positive integer,  $A \subseteq \Gamma$  such that  $\mathcal{P}_{\rho, \Omega}^{(l)}(A) > Q^{-\delta}$  for some positive integer  $l > \log Q/\delta$ , then there is  $\{a_i\}_{i=1}^{O_{\Omega}(1)} \subseteq \prod_{O_{\rho, \Omega}(1)} A$  such that*

- (1) *for any  $i$ ,  $\|\rho(a_i)\|_{S'} \leq Q^{\Theta_{\Omega, \rho}(\varepsilon)}$ , and*
- (2)  *$\prod_{\mathfrak{p} \in V_f(k') \setminus S'} [\mathcal{O}_{\mathfrak{p}}[\rho(\Gamma)] : \sum_j \mathcal{O}_{\mathfrak{p}} \rho(a_i)] \leq Q^{\varepsilon}$ . where  $\mathcal{O}_{\mathfrak{p}}[\rho(\Gamma)]$  is the  $\mathcal{O}_{\mathfrak{p}}$ -span of  $\rho(\Gamma)$ .*

For the rest of this section, let  $\Omega$  and  $\Gamma$  be as in Section 2.6, and let  $\mathbb{G}_1, \mathbb{G}_{1, \mathfrak{p}}$  be as in Section 2.4.

We need to work with normalized norms on number fields in order to have product formula. In the Appendix, the needed definition of the  $\mathfrak{p}$ -norm on a number field  $k'$  is recalled.

**Lemma 41.** *Let  $v_1, \dots, v_m \in \mathcal{O}_{k'}(S')^d \setminus \{0\}$ . Then*

$$\prod_{\mathfrak{p} \in V_f(k') \setminus S'} |(\mathcal{O}_{\mathfrak{p}}^d \cap \sum_i k'_{\mathfrak{p}} v_i) / \sum_i \mathcal{O}_{\mathfrak{p}} v_i| \ll_{d, [k':\mathbb{Q}]} \prod_i \|v_i\|_{S'}^{(|S'| + [k':\mathbb{Q}])[k':\mathbb{Q}]}.$$

*Proof.* For  $\mathcal{O}_{k'}(S')$ -submodule  $M$  of  $\mathcal{O}_{k'}(S')^d$ , let

$$c_{S'}(M) := \prod_{\mathfrak{p} \in V_f(k') \setminus S'} |(\mathcal{O}_{\mathfrak{p}}^d \cap k'[M]) / \mathcal{O}_{\mathfrak{p}}[M]|.$$

So if  $k'[M_1] = k'[M_2]$  and  $M_1 \subseteq M_2$ , then  $c_{S'}(M_1) \geq c_{S'}(M_2)$ . Hence, since  $\|v\|_{S'} \geq 1$  for any  $v \in \mathcal{O}_{k'}(S') \setminus \{0\}$ , without loss of generality we can and will assume that  $v_1, \dots, v_m$  are linearly independent over  $k'$ . Let  $X$  be the  $d$ -by- $m$  matrix having  $v_1, \dots, v_m$  on its columns. So it is a full-rank matrix. Without loss of generality we can and will assume that the first  $m$  rows are linearly independent. Let  $\text{Pr}$  be the projection onto the first  $m$  components. So the restriction of  $\text{Pr}$  to  $\sum_i k' v_i$  is injective, which implies that

$$|(\mathcal{O}_{\mathfrak{p}}^d \cap \sum_i k'_{\mathfrak{p}} v_i) / \sum_i \mathcal{O}_{\mathfrak{p}} v_i| \leq |\mathcal{O}_{\mathfrak{p}}^m / \sum_i \mathcal{O}_{\mathfrak{p}} \text{Pr}(v_i)|,$$

and so  $c_{S'}(\sum_i \mathcal{O}_{k'}(S') v_i) \leq c_{S'}(\sum_i \mathcal{O}_{k'}(S') \text{Pr}(v_i))$ . Hence, since  $\|\text{Pr}(v)\|_{S'} \leq \|v\|_{S'}$  for any  $v \in \mathcal{O}_{k'}(S')^d$ , without loss of generality we can and will assume that  $m = d$ , i.e.  $v_i$ 's span  $k'^d$ . Thus  $X \in \text{GL}_d(k') \cap M_d(\mathcal{O}_k(S'))$ . Therefore, for any  $\mathfrak{p} \in V_f(k') \setminus S'$ , there are matrices  $K_1, K_2 \in \text{GL}_d(\mathcal{O}_{\mathfrak{p}})$  and non-negative integers  $n_1, \dots, n_d$  such that

$$X = K_1 \text{diag}(\mathfrak{p}^{n_1}, \dots, \mathfrak{p}^{n_d}) K_2.$$

Hence we have

$$\begin{aligned} [\mathcal{O}_{\mathfrak{p}}^d : X(\mathcal{O}_{\mathfrak{p}}^d)] &= [K_1^{-1}(\mathcal{O}_{\mathfrak{p}}^d) : \text{diag}(\mathfrak{p}^{n_1}, \dots, \mathfrak{p}^{n_d}) K_2(\mathcal{O}_{\mathfrak{p}}^d)] \\ &= [\mathcal{O}_{\mathfrak{p}}^d : \text{diag}(\mathfrak{p}^{n_1}, \dots, \mathfrak{p}^{n_d})(\mathcal{O}_{\mathfrak{p}}^d)] \\ (29) \quad &= |\mathfrak{f}_{\mathfrak{p}}|^{\sum_i n_i}. \end{aligned}$$

On the other hand,

$$\begin{aligned} |\det(X)|_{\mathfrak{p}} &= |\det(K_1 \text{diag}(\mathfrak{p}^{n_1}, \dots, \mathfrak{p}^{n_d}) K_2)|_{\mathfrak{p}} \\ &= |\det(\text{diag}(\mathfrak{p}^{n_1}, \dots, \mathfrak{p}^{n_d}))|_{\mathfrak{p}} \\ (30) \quad &= (|\mathfrak{f}_{\mathfrak{p}}|^{-\sum_i n_i})^{1/[k':\mathbb{Q}]}. \end{aligned}$$

Therefore by Equations (29) and (30), we have

$$c_{S'}(\sum_i \mathcal{O}_{k'}(S') v_i) = \prod_{\mathfrak{p} \in V_f(k') \setminus S'} [\mathcal{O}_{\mathfrak{p}}^d : X(\mathcal{O}_{\mathfrak{p}}^d)] = \prod_{\mathfrak{p} \in V_f(k') \setminus S'} |\det(X)|_{\mathfrak{p}}^{-[k':\mathbb{Q}]}.$$

Thus by product formula we have

$$\begin{aligned} c_{S'}(\sum_i \mathcal{O}_{k'}(S') v_i) &= \prod_{\mathfrak{p} \in V_{\infty}(k') \cup S'} |\det(X)|_{\mathfrak{p}}^{[k':\mathbb{Q}]} \\ &\leq \left( \prod_{\mathfrak{p} \in V_{\infty}(k')} (d!) \prod_i \|v_i\|_{\mathfrak{p}} \right)^{[k':\mathbb{Q}]} \left( \prod_{\mathfrak{p} \in S'} \prod_i \|v_i\|_{\mathfrak{p}} \right)^{[k':\mathbb{Q}]} \\ &\leq (d!)^{[k':\mathbb{Q}]^2} \prod_i \|v_i\|_{S'}^{(|S'| + [k':\mathbb{Q}])[k':\mathbb{Q}]}. \end{aligned}$$

□

The next lemma shows that, if the probability of hitting  $A$  in  $l$ -steps is at least  $e^{-\delta l}$ , then elements with *small* logarithmic height in  $A.A$  generate a Zariski-dense subgroup of  $\mathbb{G}_1$ .



**Lemma 42.** *Let  $0 < \delta \ll_{\Omega} \varepsilon < 1$ . Let  $Q$  be a positive integer. If  $\mathcal{P}_{\Omega}^{(l)}(A) > Q^{-\delta}$  for some positive integer  $l > \log Q/\delta$  and  $Q^{\varepsilon} \gg_{\Omega} 1$ , then the group generated by  $A \cdot A \cap B_{[\varepsilon \log Q]}$  is Zariski-dense in  $\mathbb{G}_1$ , where  $B_r$  is the ball of radius  $r$  in  $\Gamma$  with respect to the  $\Omega$ -word metric.*

*Proof.* If  $\frac{1}{\delta} \log Q \geq \varepsilon' \log Q$ , then by Lemma 6 and  $\mathcal{P}_{\Omega}^{(l)}(A) > Q^{-\delta}$  we have that

$$(31) \quad \mathcal{P}_{\Omega}^{[\varepsilon' \log Q]}(A.A) \geq e^{-2\delta \log Q}.$$

Now if  $\delta_0 := \delta_0(\Omega)$  and  $l_0 := l_0(\Omega)$  are as in Proposition 18,  $\delta \leq \delta_0 \varepsilon'$  and  $[\varepsilon' \log Q] \geq l_0$ , then by Equation (31) and Proposition 18 we have that the group generated by

$$A \cdot A \cap B_{[\varepsilon' \log Q]}$$

is Zariski-dense in  $\mathbb{G}_1$ .  $\square$

**Lemma 43.** *Let  $F$  be a field,  $G$  be a subgroup of  $\mathrm{GL}_n(F)$ , and  $1 \in A \subseteq G$  be a symmetric subset which generates a Zariski-dense subgroup of  $G$ . Then*

$$\sum_{a \in \prod_{n^2} A} Fa = F[G],$$

where  $F[G]$  is the  $F$ -span of  $G$ .

*Proof.* Since  $A$  generates a Zariski-dense subgroup, the  $F$ -algebra generated by  $A$  is equal to  $F[G]$ . As  $\dim_F F[G] \leq n^2$ , the  $F$ -span of  $\prod_{n^2} A$  is equal to  $F[G]$ .  $\square$

*Proof of Proposition 40.* By Lemma 42 and Lemma 43, there are  $\{\gamma_i\}_{i=1}^{O_{\dim \rho}(1)} \subseteq \prod_{\dim \rho^2} (A.A \cap B_{[\varepsilon \log Q]})$  such that  $k'[\rho(\Gamma)] = \sum_i k' \rho(\gamma_i)$ . So in particular  $\log \|\rho(\gamma_i)\|_S \ll_{\rho, \Omega} \varepsilon \log Q$ , which implies that

$$M_d(\mathcal{O}_{\mathfrak{p}}) \cap k'_{\mathfrak{p}}[\rho(\Gamma)] = M_d(\mathcal{O}_{\mathfrak{p}}) \cap \sum_i k'_{\mathfrak{p}} \rho(\gamma_i) \supseteq \mathcal{O}_{\mathfrak{p}}[\rho(\Gamma)],$$

for any  $\mathfrak{p} \in V_f(k') \setminus S$ . Therefore we have

$$\begin{aligned} \log \prod_{\mathfrak{p} \in V_f(k') \setminus S} [\mathcal{O}_{\mathfrak{p}}[\rho(\Gamma)] : \sum_i \mathcal{O}_{\mathfrak{p}} \rho(\gamma_i)] &= \sum_{\mathfrak{p} \in V_f(k') \setminus S} \log[(\mathcal{O}_{\mathfrak{p}}[\rho(\Gamma)] : \sum_i \mathcal{O}_{\mathfrak{p}} \rho(\gamma_i))] \\ &\leq \sum_{\mathfrak{p} \in V_f(k') \setminus S} \log[M_d(\mathcal{O}_{\mathfrak{p}}) \cap \sum_i k'_{\mathfrak{p}} \rho(\gamma_i) : \sum_i \mathcal{O}_{\mathfrak{p}} \rho(\gamma_i)] \end{aligned}$$

$$\text{(By Lemma 41)} \quad \ll_{\dim \rho, [k':\mathbb{Q}], |S|} \sum_i \log \|\rho(\gamma_i)\|_S$$

$$\text{(for } Q^{\varepsilon} \gg_{\Omega, \rho} 1) \quad \ll_{\Omega, \rho} \varepsilon \log Q.$$

$\square$

**4.2. Large number of conjugacy classes.** In this section, by the virtue of the proof of Burnside theorem, we prove the following proposition.

**Proposition 44.** *Let  $\Omega, \Gamma$  (we might pass to a subgroup of finite-index using Lemma 20),  $\mathbb{G}_1$ , and  $\mathbb{G}_{1, \mathfrak{p}}$  be as before, and let  $\pi_Q$  be as in the beginning of Section 3.1. And suppose  $0 < \delta \ll_{\Omega} \varepsilon \ll_{\Omega} 1$  and  $1 \ll_{\Omega} \varepsilon \log_p Q$ .*

*If  $\mathcal{P}_{\Omega}^{(l)}(A) > Q^{-\delta}$  for some positive integer  $l > \log Q/\delta$ , then there is  $\{a_i\}_{i=1}^{O_{\Omega}(1)} \subseteq \prod_{O_{\Omega}(1)} A$  such that for any positive integer  $n \gg_{\Omega} \varepsilon \log_p Q$  there is a positive integer  $n'$  with the following properties:*

$$(1) \quad n' \leq n \leq n' + \varepsilon \log_p Q,$$

(2) For any  $X \subseteq \Gamma$ , there is an  $i$  such that

$$|\pi_{q'}(X)|^{\Theta_\Omega(1)} \leq |\text{Conj}(\pi_q(Xa_i))|,$$

where  $q := p^n$ ,  $q' := p^{n'}$ , and  $\text{Conj}(Y) = \{[y] \mid y \in Y\}$  where  $[y]$  is the intersection of the conjugacy class of  $y$  and  $Y$ .

One can deduce Proposition 44 from the following proposition.

**Proposition 45.** *In the above setting, suppose  $0 < \delta \ll_\Omega \varepsilon \ll_\Omega 1$  and  $1 \ll_\Omega \varepsilon \log_p Q$ . Suppose  $p \in V_f(\mathbb{Q})$  and  $\mathfrak{p} \mid p$  for some  $\mathfrak{p} \in V_f(k) \setminus S$ .*

*If  $\mathcal{P}_\Omega^{(l)}(A)$  for some positive integer  $l > \log Q/\delta$ , then there is  $\{a_i\}_{i=1}^{O_\Omega(1)} \subseteq \prod_{O_\Omega(1)} A$  such that for any positive integer  $n \gg_\Omega \varepsilon \log_p Q$ , there is a positive integer  $n'$  with the following properties:*

- (1)  $n' \leq n \leq n' + \varepsilon \log_p Q$ ,
- (2) For any  $\gamma \in \Gamma$ , let  $\Xi_q(\gamma) := (\mathcal{C}(\pi_q(\gamma a_i)))_i$ , where  $q := p^n$  and  $\mathcal{C}(y)$  is the conjugacy class of  $y$ . If  $\Xi_q(\gamma_1) = \Xi_q(\gamma_2)$ , then  $\pi_{q'}(\gamma_1) = \pi_{q'}(\gamma_2)$  where  $q' := p^{n'}$ .

*Proof.* Recall from Section 2.6 that  $\Gamma \subseteq \text{GL}_{n_0}(\mathcal{O}_k(S))$ , and  $S_0 := \{p \in V_f(\mathbb{Q}) \mid \exists \mathfrak{p} \in S, \mathfrak{p} \mid p\}$ . Moreover  $\mathbb{G}_1$  is a  $\mathbb{Q}$ -semisimple group, and  $\mathbb{G}_{1,\mathfrak{p}}$  is a factor of  $\mathbb{G}_1$  that is defined over a subfield  $k(\mathfrak{p})$  of  $k$ . So there are absolutely irreducible representations  $\rho_i : \mathbb{G} \rightarrow \text{GL}_{n_i}$  that are defined over a Galois extension  $k'$  of  $k$ , and  $\rho = \oplus_{i \in I} \rho_i$  is a faithful representation. Furthermore we can and will assume that for any  $\mathfrak{p} \in \{\mathfrak{p} \in V_f(k) \setminus S \mid \exists p \in S_0, \mathfrak{p} \mid p\}$  there is a subset  $I_{\mathfrak{p}}$  of  $I$  such that  $\rho_i$  factors through  $\mathbb{G}_{1,\mathfrak{p}}$  for any  $i \in I_{\mathfrak{p}}$  and  $\oplus_{i \in I_{\mathfrak{p}}} \rho_i$  induces a faithful representation of  $\mathbb{G}_{1,\mathfrak{p}}$ . We consider  $\rho_i$ 's fixed and do not mention the dependence of constants to the choice of such homomorphisms. Let

$$\mathcal{C}_i := \{\tilde{\mathfrak{p}} \in V_f(k') \mid \rho_i(\Gamma) \text{ is a bounded subgroup of } \text{GL}_{n_i}(k'_{\tilde{\mathfrak{p}}})\}.$$

So we have that  $\{\tilde{\mathfrak{p}} \in V_f(k') \mid \exists p \in V_f(\mathbb{Q}) \setminus S_0, \tilde{\mathfrak{p}} \mid p\} \subseteq \mathcal{C}_i$  for any  $i \in I$ . And for any  $\mathfrak{p} \in V_f(k) \setminus S$  and  $i \in I_{\mathfrak{p}}$  we have  $\{\tilde{\mathfrak{p}} \in V_f(k') \mid \tilde{\mathfrak{p}} \mid \mathfrak{p}\} \subseteq \mathcal{C}_i$ .

Let  $S_i := V_f(k') \setminus \mathcal{C}_i$ . By Lemma 20 and Lemma 12, we can assume that

$$\rho_i(\Gamma) \subseteq \text{GL}_{n_i}(\mathcal{O}_{k'}(S_i)).$$

Therefore by Proposition 40, there is  $\{a_i\}_{i=1}^{O_\Omega(1)} \subseteq \prod_{O_\Omega(1)} A$  such that for any  $i \in I$  and  $j$

$$(32) \quad \|\rho_i(a_j)\|_{S_i} \leq Q^{\Theta_\Omega(\varepsilon)},$$

and

$$(33) \quad \prod_{\tilde{\mathfrak{p}} \in \mathcal{C}_i} |\mathcal{O}_{\tilde{\mathfrak{p}}}[\rho_i(\Gamma)]| / \sum_j |\mathcal{O}_{\tilde{\mathfrak{p}}}(\rho_i(a_j))| \leq Q^\varepsilon.$$

Since  $\rho_i$  is absolutely irreducible, we have  $k'[\rho_i(\Gamma)] = M_{n_i}(k')$ . By (33), there is a subset  $J_i$  of indexes such that  $\{\rho_i(a_j)\}_{j \in J_i}$  is a  $k'$ -basis of  $M_{n_i}(k')$ . Let  $T_i : M_{n_i}(k') \rightarrow k'^{n_i^2}$  be

$$T_i(x) := (\text{Tr}(x \rho_i(a_j)))_{j \in J_i}.$$

Since  $f_i : M_{n_i}(k') \times M_{n_i}(k') \rightarrow k'$ ,  $f_i(x, y) := \text{Tr}(x, y)$  is a  $k'$ -bilinear non-degenerate map,  $T_i$  is an invertible  $k'$ -linear map. Moreover the matrix representation of  $T_i$  in the standard basis of  $M_{n_i}(k')$  has entries in  $\mathcal{O}_{k'}(S_i)$ , and by (32), the  $S_i$ -norm of its entries are at most  $Q^{\Theta_\Omega(\varepsilon)}$ . Hence by product formula we have

$$(34) \quad |\det(T_i)|_{\tilde{\mathfrak{p}}} \leq 1, \text{ and } \prod_{\tilde{\mathfrak{p}} \in \mathcal{C}_i} |\det(T_i)|_{\tilde{\mathfrak{p}}} \geq Q^{-\Theta_\Omega(\varepsilon)}.$$

For any  $\mathfrak{p} \in V_f(k) \setminus S$  and  $\tilde{\mathfrak{p}} \in V_f(k')$  which divides  $\mathfrak{p}$  we have

$$(35) \quad \|g_1 - g_2\|_{\tilde{\mathfrak{p}}} \ll \max_{i \in I_{\mathfrak{p}}} \|\rho_i(g_1) - \rho_i(g_2)\|_{\tilde{\mathfrak{p}}} \ll \|g_1 - g_2\|_{\tilde{\mathfrak{p}}},$$

for any  $g_1, g_2 \in \mathbb{G}_{1,\mathfrak{p}}(\mathbb{Z}_p)$ , since  $\oplus_{i \in I_{\mathfrak{p}}} \rho_i$  induces an injective homomorphism on  $\mathbb{G}_{1,\mathfrak{p}}$ .

Suppose  $\mathfrak{p} \in V_f(k) \setminus S$  divides  $p \in V_f(\mathbb{Q})$ ,  $q = p^n$ , and  $\Xi_q(\gamma_1) = \Xi_q(\gamma_2)$ . Then for any  $j$  we have that  $\|\gamma_1 a_j - g_j \gamma_2 a_j g_j^{-1}\|_{\mathfrak{p}} \leq |q|_{\mathfrak{p}}$  for some  $g_j \in \Gamma$ . Therefore for any  $i$  and  $j$  and any  $\tilde{\mathfrak{p}} \in V_f(k')$  that divides  $\mathfrak{p}$  we have

$$(36) \quad \begin{aligned} |\mathrm{Tr}(\rho_i(\gamma_1 a_j)) - \mathrm{Tr}(\rho_i(\gamma_2 a_j))|_{\tilde{\mathfrak{p}}} &= |\mathrm{Tr}(\rho_i(\gamma_1 a_j) - \rho_i(g_j \gamma_2 a_j g_j^{-1}))|_{\tilde{\mathfrak{p}}} \\ &\ll \|\gamma_1 a_j - g_j \gamma_2 a_j g_j^{-1}\|_{\tilde{\mathfrak{p}}} \leq |q|_{\tilde{\mathfrak{p}}}. \end{aligned}$$

So by (36) for any  $i$  we have

$$(37) \quad \|T_i(\rho_i(\gamma_1)) - T_i(\rho_i(\gamma_2))\|_{\tilde{\mathfrak{p}}} \ll |q|_{\tilde{\mathfrak{p}}}.$$

Hence by (34) and (37) we have

$$(38) \quad \|\rho_i(\gamma_1) - \rho_i(\gamma_2)\|_{\tilde{\mathfrak{p}}} \leq Q^{\Theta_{\Omega}(\varepsilon)} |q|_{\tilde{\mathfrak{p}}}.$$

Therefore by (35) we have

$$\|\gamma_1 - \gamma_2\|_{\tilde{\mathfrak{p}}} \leq Q^{\Theta_{\Omega}(\varepsilon)} |q|_{\tilde{\mathfrak{p}}},$$

which implies that  $\pi_{q'}(\gamma_1) = \pi_{q'}(\gamma_2)$  for some  $q'|q$  and  $q' \geq qQ^{-\Theta_{\Omega}(\varepsilon)}$ .  $\square$

**4.3. Helfgott's trick to get large centralizer.** In this section, we recall Helfgott's method of getting a large centralizer and prove the following lemma.

**Lemma 46.** *Let  $\Omega$  and  $\Gamma$  be as in Section 2.6, and let  $\pi_{p^n}$  be as in Section 3.1. Assume  $0 < \delta \ll_{\Omega} \varepsilon \ll_{\Omega} 1$  and  $1 \ll_{\Omega} \varepsilon N$  where  $N$  is a positive integer. Suppose  $p$  is divisible by some  $\mathfrak{p} \in V_f(k) \setminus S$ .*

*Suppose  $\mathfrak{P}_Q(\delta, A, l)$  holds, where  $Q := p^N$ , and  $\{a_i\}_{i=1}^{O_{\Omega}(1)} \subseteq \prod_{O_{\Omega}(1)} A$  is as in Proposition 44. Then for any  $X \subseteq \prod_{O_{\Omega}, \varepsilon(1)} A$  and for any integer  $N\varepsilon \ll_{\Omega} n \leq N$  there are  $i, x \in Xa_i$ , and a positive integer  $n'$  such that*

- (1)  $n' \leq n \leq n' + \varepsilon N$ ,
- (2)  $|C_{\pi_q(\Gamma)}(\pi_q(x)) \cap \pi_q(A \cdot A)| \geq |\pi_Q(A)|^{-\Theta_{\Omega}, \varepsilon(\delta)} |\pi_{q'}(X)|^{\Theta_{\Omega}(1)}$ , where  $q := p^n$  and  $q' := p^{n'}$ .

One can deduce Lemma 46 from Proposition 44 and the following lemma.

**Lemma 47.** *In the above setting. Assume  $0 < \delta \ll_{\Omega} \varepsilon \ll_{\Omega} 1$  and  $1 \ll_{\Omega} \varepsilon N$  where  $N$  is a positive integer. Suppose  $p$  is divisible by some  $\mathfrak{p} \in V_f(k) \setminus S$ .*

*Suppose that  $\mathfrak{P}_Q(\delta, A, l)$  holds, where  $Q := p^N$ , and  $\{a_i\}_{i=1}^{O_{\Omega}(1)} \subseteq \prod_{O_{\Omega}(1)} A$  is as in Proposition 44. Then for any  $i$  and any  $X \subseteq \prod_{O_{\Omega}, \varepsilon(1)} A$  and for any  $q|Q$  there is  $x_0 \in X$  such that*

$$|C_{\pi_q(\Gamma)}(\pi_q(x_0 a_i)) \cap \pi_q(A \cdot A)| \geq |\pi_Q(A)|^{-\Theta_{\Omega}, \varepsilon(\delta)} |\mathrm{Conj}(\pi_q(X a_i))|.$$

*Proof.* Since  $|\pi_Q(A)|^{1+\delta} \geq |\pi_Q(\prod_3 A)|$ , for any  $q|Q$  we have that

$$(39) \quad |\pi_q(A)| |\pi_Q(A)|^{\delta} \geq |\pi_q(\prod_3 A)|.$$

Therefore by the Ruzsa-inequality we have that  $|\pi_q(\prod_{O_{\Omega}, \varepsilon(1)} A)| \leq |\pi_Q(A)|^{\Theta_{\Omega}, \varepsilon(\delta)} |\pi_q(A)|$ .

For any  $X \subseteq \prod_{O_{\Omega}, \varepsilon(1)} A$  and  $i$  we have that

$$(40) \quad |\pi_q(\prod_{O_{\Omega}, \varepsilon(1)} A)| \geq |\pi_q(A X a_i A)|$$

$$(41) \quad \geq \sum_{[\pi_q(x)] \in \mathrm{Conj}(\pi_q(X a_i))} |\{\pi_q(a x a^{-1}) \mid a \in A\}|$$

$$(42) \quad \geq |\pi_q(A)| \cdot |\mathrm{Conj}(\pi_q(X a_i))| \cdot \mathbb{E}_{[\pi_q(x)]} \left( \frac{1}{|C_{\pi_q(\Gamma)}(\pi_q(x)) \cap \pi_q(A \cdot A)|} \right).$$

So for some  $x_0 \in X$  we have that

$$(43) \quad |C_{\pi_q(\Gamma)}(\pi_q(x_0 a_i)) \cap \pi_q(A \cdot A)| \geq \frac{|\pi_q(A)|}{|\pi_q(\prod_{O_{\Omega, \varepsilon}(1)} A)|} \cdot |\text{Conj}(\pi_q(X a_i))|.$$

□

**4.4. Measuring the regularity.** In this section, we recall what a *regular semisimple* element is, and we describe a way to measure *how much* regular semisimple an element is. Let  $K$  be a local non-archimedean field,  $|\cdot|$  its norm,  $\mathcal{O}$  its ring of integers, and  $\mathfrak{p}$  a uniformizing element. Let  $\mathbb{H}$  be a connected semisimple  $K$ -group, and let  $r$  be the absolute rank of  $\mathbb{H}$ . Steinberg [Ste65, Corollary 6.8] proved that there is  $h_s \in K[\mathbb{H}]$  such that

- (1)  $h_s(g) = F_g(1)$ , where  $F_g(x)(x-1)^r := \det(\text{Ad}(g) - xI)$ ,
- (2)  $g \in \mathbb{G}(\overline{K})$  is *regular semisimple* if and only if  $h_s(g) \neq 0$ .

**Definition 48.** Let  $\mathcal{H}$  be an  $\mathcal{O}$ -subscheme of  $(\mathcal{GL}_n)_{\mathcal{O}}$ . Suppose the generic fiber  $\mathbb{H}$  of  $\mathcal{H}$  is a connected semisimple  $K$ -group. Let  $f_s \in \mathcal{O}[\mathcal{H}]$  be

$$f_s(g) = R\left((x-1)F_g(x), \frac{d}{dx}((x-1)F_g(x))\right),$$

where  $R(f_1, f_2)$  is the resultant of  $f_1$  and  $f_2$ . For  $\eta > 0$ , we say  $g \in \mathcal{H}(\mathcal{O})$  is  $\eta$ -regular semisimple if  $|f_s(g)| > \eta$ . Equivalently  $g \in \mathcal{H}(\mathcal{O})$  is  $|q|$ -regular semisimple if and only if  $\pi_q(f_s(g)) \neq 0$ .

**Remark 49.** If  $R$  is any integral domain and  $\mathcal{H}$  is an  $R$ -subscheme of  $(\mathcal{GL}_n)_R$  with a connected semisimple generic fiber  $\mathbb{H}$ , then  $f_s \in R[\mathcal{H}]$  can be defined in the same way.

Before summarizing the basic properties of  $\eta$ -regular semisimple elements, an elementary lemma on certain diagonalizable elements of  $\text{GL}_n(\mathcal{O})$  is proved.

**Lemma 50.** Suppose  $a \in \text{GL}_n(\mathcal{O})$  is diagonalizable over  $K$  and let  $\lambda_i$  be its distinct eigenvalues (which are not necessarily of multiplicity one). Assume that  $\prod_{i \neq j} (\lambda_i - \lambda_j) \in \mathfrak{p}^m \mathcal{O} \setminus \mathfrak{p}^{m+1} \mathcal{O}$ . Then

$$\mathfrak{p}^m \mathcal{O}^n \subseteq \bigoplus_i (V_{\lambda_i} \cap \mathcal{O}^n),$$

where  $V_{\lambda_i} := \{\mathbf{v} \in K^n \mid a\mathbf{v} = \lambda_i \mathbf{v}\}$ .

*Proof.* Since  $a$  is diagonalizable, we have that  $K^n = \bigoplus_i V_{\lambda_i}$ . So for any  $\mathbf{x} \in \mathcal{O}^n$  there are  $\mathbf{x}_i \in V_{\lambda_i}$  such that  $\mathbf{x} = \sum_i \mathbf{x}_i$ . Therefore for any integer  $j$  we have  $a^j \mathbf{x} = \sum_i \lambda_i^j \mathbf{x}_i \in \mathcal{O}^n$ . Since  $a \in \text{GL}_n(\mathcal{O})$  and it is diagonalizable over  $K$ , all the eigenvalues  $\lambda_i$  are in  $\mathcal{O}$ . Hence by the Vandermonde equality we have that  $\prod_{i \neq j} (\lambda_i - \lambda_j) \mathbf{x}_k \in \mathcal{O}^n$  for any  $k$ , which implies that

$$\mathfrak{p}^m \mathcal{O}^n \subseteq \bigoplus_i (V_{\lambda_i} \cap \mathcal{O}^n).$$

□

**Lemma 51.** In the above setting, let  $g \in \mathcal{H}(\mathcal{O})$ ,  $q \in \mathfrak{p}\mathcal{O}$ , and  $\eta := |q|$ . Suppose  $h$  is  $\eta$ -regular semisimple. Then

- (1)  $\mathbb{T} := C_{\mathbb{G}}(g)^{\circ}$  is a maximal  $K$ -torus of  $\mathbb{H}$ .
- (2)  $g \in \mathbb{T}(K)$ .
- (3) There is a Galois extension  $K'$  of  $K$  such that  $[K' : K] \leq n!$ , and  $\text{Ad}(\mathbb{T})$  splits over  $K'$ . In particular,

$$\mathfrak{h}(K') = \mathfrak{t}(K') \oplus \bigoplus_{\phi \in \Phi(\mathbb{H}, \mathbb{T})} \mathfrak{h}_{\phi}(K'),$$

where  $\mathfrak{h} := \text{Lie}(\mathcal{H})$ ,  $\mathbb{T} = \text{Lie}(\mathbb{T})$ ,  $\Phi(\mathbb{H}, \mathbb{T})$  is the set of weights of the adjoint representation with respect to  $\mathbb{T}$  and  $\mathfrak{h}_\phi$  are the corresponding weight spaces. In this setting, we have

$$\begin{aligned} h_s(g) &= \prod_{\phi \in \Phi(\mathbb{H}, \mathbb{T})} (\phi(g) - 1) \\ f_s(g) &= \pm h_s(g)^2 \cdot \prod_{\phi_1 \neq \phi_2 \in \Phi(\mathbb{H}, \mathbb{T})} (\phi_1(g) - \phi_2(g))^2 \notin q\mathcal{O}', \end{aligned}$$

where  $\mathcal{O}'$  is the ring of integers of  $K'$ .

- (4)  $g' \in \mathcal{H}(\mathcal{O})$  is  $|q|^{O_n(1)}$ -regular semisimple if and only if for any distinct roots  $\phi$  and  $\phi'$

$$|\phi(g') - 1| \geq |q|^{O_n(1)}, \text{ and } |\phi(g') - \phi'(g')| \geq |q|^{O_n(1)},$$

for suitable choice of the implied constants.

- (5) We have

$$q\mathfrak{h}(\mathcal{O}') \subseteq (\mathfrak{h}(\mathcal{O}') \cap \mathfrak{t}(K')) \oplus \bigoplus_{\phi \in \Phi(\mathbb{H}, \mathbb{T})} (\mathfrak{h}(\mathcal{O}') \cap \mathfrak{h}_\phi(K')).$$

And so, for  $q' \in q^2\mathcal{O}$  and  $x \in \mathfrak{h}(\mathcal{O}')$ , if  $\text{Ad}(g)(x) = x \pmod{q'}$ , then

$$x \equiv h \pmod{q'/q^2},$$

for some  $h \in \mathfrak{h}(\mathcal{O}') \cap \mathfrak{t}(K')$ .

*Proof.* Since  $F_g(x)$  is a monic polynomial,  $f_s(x)$  is, up to a sign, the discriminant of  $(x-1)F_g(x)$ . Therefore, if  $f_s(g)$  is non-zero, then  $h_s(g)$  is non-zero. And so  $g$  is a regular semisimple element. This implies Part (1). Part (2) is a well-known consequence of Part (1) (see [Hum95, Chapter 22.3]). Parts (3) and (4) can easily be deduced from the definitions and the earlier argument. The first claim of Part (5) is a direct consequence of Lemma 50 and Part (3). For any  $x \in \mathfrak{h}(\mathcal{O}')$  there are  $h' \in \mathfrak{h}(\mathcal{O}') \cap \mathfrak{t}(K')$  and  $x_\phi \in \mathfrak{h}(\mathcal{O}') \cap \mathfrak{g}_\phi(K')$  such that  $qx = h' + \sum_{\phi \in \Phi(\mathbb{H}, \mathbb{T})} x_\phi$ . Hence

$$\text{Ad}(g)(qx) - (qx) = \sum_{\phi \in \Phi(\mathbb{H}, \mathbb{T})} (\phi(g) - 1)x_\phi = qq'y,$$

for some  $y \in \mathfrak{h}(\mathcal{O}')$ . Again using the first claim of Part (5) we know that there are  $y_\phi \in \mathfrak{h}(\mathcal{O}') \cap \mathfrak{h}_\phi(K')$  such that  $qy = \sum_{\phi} y_\phi$ . Hence for any  $\phi \in \Phi(\mathbb{H}, \mathbb{T})$  we have  $(\phi(g) - 1)x_\phi = q'y_\phi$ . On other hand, by Part (3), we have that  $|\phi(g) - 1| > |q|$ . Therefore  $x_\phi \in (q'/q)\mathfrak{h}(\mathcal{O}')$ , which implies the second claim of Part (5).  $\square$

**Lemma 52.** Let  $\Omega$  and  $\Gamma$  be as in Section 2.6, and  $\mathcal{G}_1$ ,  $\mathcal{G}_{1,\mathfrak{p}}$ , and  $\pi_{p^n}$  be as in Section 3.1. Let  $\mathfrak{p} \in V_f(k) \setminus S$  which divides  $p \in V_f(\mathbb{Q})$ . Let the triple of a group scheme  $\mathcal{H}$ , a number field  $k'$ , and a norm  $|\cdot|_\nu$  of  $k'$  be either  $(\mathcal{G}_1, \mathbb{Q}, |\cdot|_p)$  if  $p \notin S_0$ , or  $(\mathcal{G}_{1,\mathfrak{p}}, k(\mathfrak{p}), |\cdot|_\mathfrak{p})$  if  $p \in S_0$ .

Suppose  $q, q_0, q_1, q_2$  are powers of  $p$ ,  $q_1|q_2$ ,  $q_0q^2q_2|q_1^2$ , and  $\log_p q_0 \gg_n 1$  and  $\log_p(q_1^2/(q_0q^2q_2)) \gg_\Gamma 1$ . If  $\gamma \in \Gamma \subseteq \mathcal{H}(\mathbb{Z}_p)$  is  $|q|_\nu$ -regular semisimple, then

$$\Psi_{q_1}^{q_2}(\pi_{q_2}(C_{\pi_{q_0q^2q_2}(\Gamma)}(\pi_{q_0q^2q_2}(\gamma))) \cap \pi_{q_2}(\Gamma[q_1])) \subseteq \pi_{q_2/q_1}(\text{Lie}(\mathcal{H})(\mathbb{Z}_p) \cap \mathfrak{t}(k')),$$

where  $\mathfrak{t} := \text{Lie } C_{\mathbb{H}}(\gamma)^\circ$  and  $\mathbb{H}$  is the generic fiber of  $\mathcal{H}$ .

*Proof.* Suppose  $\pi_{q_0q^2q_2}(\gamma') \in C_{\pi_{q_0q^2q_2}(\Gamma)}(\pi_{q_0q^2q_2}(\gamma))$  such that  $\pi_{q_2}(\gamma') \in \pi_{q_2}(\Gamma[q_1])$ . Therefore  $\gamma' \in \Gamma[q_1]$ . Let  $q'_3 := q_0q^2q_2/q_1$  and  $\mathfrak{h} := \text{Lie}(\mathcal{H})(\mathbb{Z}_p)$ .

Since  $\log_p(q_1^2/(q_0q^2q_2)) \gg_\Omega 1$ , by Part 2 of Lemma 29 we have that

$$\Psi_{q_1}^{q_0q^2q_2} : \pi_{q_0q^2q_2}(\Gamma[q_1]) \rightarrow \mathfrak{h}/q'_3\mathfrak{h}$$

is a  $\Gamma$ -module isomorphism between. Hence there is  $x \in \mathfrak{h}$  such that

$$\pi_{q'_3}(x) = \Psi_{q_1}^{q_0q^2q_2}(\pi_{q_0q^2q_2}(\gamma')), \quad \text{Ad}(\gamma)(x) \equiv x \pmod{q'_3}.$$

Thus by Part 5 of Lemma 51 there is a Galois extension  $k''$  of  $k'$  and  $h' \in \text{Lie}(\mathcal{H})(\mathcal{O}) \cap \text{Lie}(\mathbb{T})(k'')$  where  $\mathbb{T} := C_{\mathbb{H}}(\gamma)^\circ$  such that

$$(44) \quad [k'' : k'] \ll_n 1, \text{ and } x \equiv h' \pmod{q'_3/q^2}, \text{ i.e. } x \equiv h \pmod{q_0 q_2/q_1}.$$

(Let us recall that  $k(\mathfrak{p})$  is essentially the intersection of the copy of  $\mathbb{Q}_p$  in  $k_{\mathfrak{p}}$  and  $k$ .) So there is  $x' \in \text{Lie}(\mathcal{H})(\mathcal{O})$  such that

$$x = h' + q_0 q_3 x',$$

where  $q_3 := q_2/q_1$ . Since  $x \in \text{Lie}(\mathcal{H})(k')$ , for any  $\sigma \in \text{Gal}(k''/k')$  we have

$$h' - \sigma(h') = q_0 q_3 (\sigma(x') - x').$$

Therefore we have

$$h' = \frac{1}{[k'' : k']} \sum_{\sigma \in \text{Gal}(k''/k')} \sigma(h') + \frac{q_0 q_3}{[k'' : k']} \sum_{\sigma \in \text{Gal}(k''/k')} (\sigma(x') - x').$$

Since  $\log_p q_0 \gg_n 1$ , we have

$$x - h' \in q_3 \text{Lie}(\mathcal{H})(\mathcal{O}),$$

where  $\mathcal{O}$  is the ring of integers of a composite field of  $k''$  and  $\mathbb{Q}_p$ , and  $h := \frac{1}{[k'' : k']} \sum_{\sigma \in \text{Gal}(k''/k')} \sigma(h')$ . In particular,  $h$  is invariant under the Galois action. Since  $\mathbb{T}$  is defined over  $k'$ , we have  $h \in \text{Lie}(\mathbb{T})(k')$ . Altogether we have that

$$x - h \in q_3 \mathfrak{h}, \quad h \in \text{Lie}(\mathcal{H})(\mathbb{Z}_p) \cap \text{Lie}(\mathbb{T})(k').$$

□

**4.5. Hitting shifts of regular semisimple elements.** The main result of this Section is Proposition 53. It is essentially proved, in a *quantitative way*, that after certain *number of steps* in the random-walk there is only a *small chance* of hitting a translation by a *small* element of a not-sufficiently regular element. Of course the main issue is gaining control on the relation between the four parameters: the needed number of steps in the random-walk; the size of translation; the size of regularity; and an upper bound on the considered probability.

For the rest of this section, let  $\Omega$  and  $\Gamma$  be as in Section 2.6, and  $\mathcal{G}_1, \mathcal{G}_{1,\mathfrak{p}}$ , and  $\pi_{p^n}$  be as in Section 3.1. Let  $\mathfrak{p} \in V_f(k) \setminus S$  which divides  $p \in V_f(\mathbb{Q})$ . Let the quadruple  $(\mathcal{H}, k', \nu, S')$  of a group scheme  $\mathcal{H}$ , a number field  $k'$ , a place  $\nu \in V_f(k')$ , and a finite subset  $S'$  of  $V_f(k')$  be either  $(\mathcal{G}_1, \mathbb{Q}, p, S_0)$  if  $p \notin S_0$ , or  $(\mathcal{G}_{1,\mathfrak{p}}, k(\mathfrak{p}), \mathfrak{p}, S)$  if  $p \in S_0$ . In particular,  $\Gamma \subseteq \mathcal{H}(\mathcal{O}_{k'}(S'))$ .

**Proposition 53.** *Suppose  $0 < \varepsilon \ll_n 1$ ,  $q := p^n$ ,  $Q := p^N$  where  $n, N \in \mathbb{Z}^+$  and  $n \geq N\varepsilon$ . Let  $a \in \Gamma$  such that  $Q^\varepsilon \geq \|a\|_{S'}$  and  $l \gg_\Omega \varepsilon \log Q$ . Then*

$$\mathcal{P}_\Omega^{(l)}(\{\gamma \in \Gamma \mid \gamma a \text{ is not a } |q|_\nu - \text{regular semisimple}\}) \leq Q^{-\Theta_\Omega(\varepsilon)}.$$

To simplify the presentation, let

$$W_{a,q} := \{\gamma \in \Gamma \mid \gamma a \text{ is not a } |q|_\nu - \text{regular semisimple}\}.$$

By the definition of  $|q|_\nu$ -regular semisimple elements, we know that

$$W_{a,q} := \{\gamma \in \Gamma \mid \pi_q(f_s(\gamma a)) = 0\}.$$

And, for  $\gamma_1, \gamma_2 \in \Gamma$  and  $q_1, q_2$ , powers of  $p$ , let

$$\begin{aligned} V_{q_1, q_2}(\gamma_1, \gamma_2) &:= \{\gamma \in \Gamma \mid \gamma_1 \gamma \gamma_2 \in W_{1, q_1} \text{ and } \|\gamma\|_{S'} \leq q_2\} \\ &\quad \{\gamma \in \Gamma \mid \pi_{q_1}(f_s(\gamma_1 \gamma \gamma_2)) = 0, \|\gamma\|_{S'} \leq q_2\}. \end{aligned}$$

For  $g \in \mathbb{H}(\overline{k'})$  and  $\gamma_0 \in \Gamma$ , let  $f_{g, \gamma_0}(g') := f_s(gg'\gamma_0)$  and  $V(f_{g, \gamma_0}) \subseteq \mathbb{G}$  be the zeros of  $f_{g, \gamma_0}$ , where  $\mathbb{H}$  is the generic fiber of  $\mathcal{H}$ . The following is the key lemma in the proof of Proposition 53.

**Lemma 54.** *Let  $\gamma_1, \gamma_2 \in \Gamma$ . Suppose  $\|\gamma_2\|_{S'} \leq q_2 \leq q_1^{O_\Omega(1)}$  and  $q_2 \gg_\Omega 1$ . Then there is  $g \in \mathbb{H}(\overline{k'})$  such that  $h(g) \ll_\Omega \log q_2$ , where  $h(g)$  is the logarithmic height of  $g$ , and  $V_{q_1, q_2}(\gamma_1, \gamma_2) \subseteq V(f_{g, \gamma_2})$ .*

*Proof.* Let  $Y := \{g \in \mathbb{H}(\overline{k'}) \mid f_s(g\gamma\gamma_2) = 0 \text{ for any } \gamma \in V_{q_1, q_2}(\gamma_1, \gamma_2)\}$ . We would like to prove that there is  $g \in Y$  such that  $h(g) \ll_\Omega \log q_2$ . First we prove that  $Y \neq \emptyset$ .

Let  $Q_1(\underline{X}), \dots, Q_m(\underline{X}) \in \mathcal{O}_{k'}(S')[X_{11}, \dots, X_{nn}]$  be such that  $\mathcal{O}_{k'}(S')[\mathcal{H}] = \mathcal{O}_{k'}(S')[X_{11}, \dots, X_{nn}]/\langle Q_i \rangle$ . If  $Y = \emptyset$ , then by the effective Nullstellensatz [MW83, Theorem IV] and the fact that the logarithmic height of  $f_s(\underline{X}\gamma\gamma_2)$  is  $O_{\dim \mathbb{H}}(\log q_2)$  we have that there are

$$P_\gamma(\underline{X}), P_1(\underline{X}), \dots, P_m(\underline{X}) \in \mathcal{O}_{k'}[X_{11}, \dots, X_{nn}] \text{ and } d \in \mathcal{O}_{k'}$$

such that

- (1)  $d = \sum_{\gamma \in V_{q_1, q_2}(\gamma_1, \gamma_2)} P_\gamma(\underline{X}) f_s(\underline{X}\gamma\gamma_2) + \sum_i P_i(\underline{X}) Q_i(\underline{X})$ ,
- (2)  $\deg P_\gamma, \deg P_i \ll O_\Omega(1)$ ,
- (3)  $h(d) \ll_{\dim \mathbb{H}} \log q_2$ .

Therefore  $d = \sum_{\gamma \in V_{q_1, q_2}(\gamma_1, \gamma_2)} P_\gamma(\gamma_1) f_s(\gamma_1\gamma\gamma_2)$  and so  $d \in q_1 \mathcal{O}_{k'}(S')$ . Therefore

$$\log |d|_\nu \leq \log |q_1|_\nu \ll_{\deg k'} -\log q_1$$

as  $\nu \notin S'$ . Thus we have

$$\begin{aligned} \log q_2 \gg_{\dim \mathbb{H}} h(d) &= \sum_{\nu' \in V_\infty(k')} \log^+ |d|_{\nu'} \geq \sum_{\nu' \in V_\infty(k')} \log |d|_{\nu'} \\ (\text{product formula}) &= - \sum_{\nu' \in V_f(k')} \log |d|_{\nu'} \geq -\log |d|_\nu \gg_{\deg k'} \log q_1. \end{aligned}$$

This contradicts the assumption  $q_2 \leq q_1^{O_\Omega(1)}$ . And so  $Y \neq \emptyset$ .

Now by Proposition 66 we know  $Y$  has a point with *small* height, i.e. there is  $g \in \mathbb{G}(\overline{\mathbb{Q}})$  such that  $V_{q_1, q_2}(\gamma_1, \gamma_2) \subseteq V(f_{g, \gamma_2})$  and  $H(g) \leq q_2^{O_\Omega(1)}$ .  $\square$

**Corollary 55.** *Let  $\gamma_1, \gamma_2 \in \Gamma$ . Suppose  $\|\gamma_2\|_{S'} \leq q_2 \leq q_1^{O_\Omega(1)}$  and  $q_2 \gg_\Omega 1$ . Then*

$$\mathcal{P}_\Omega^{(l)}(V_{q_1, q_2}(\gamma_1, \gamma_2)) \ll q_2^{-O_\Omega(1)},$$

where  $l \gg_\Omega \log q_2$ .

*Proof.* By Lemma 54, there is  $g \in \mathbb{H}(\overline{k'})$  such that  $V_{q_1, q_2}(\gamma_1, \gamma_2) \subseteq V(f_{g, \gamma_2})$  and  $h(g) \ll_\Omega \log q_2$ . By Corollary 23 we have  $p_0(V(f_{g, \gamma_2})) \ll_\Omega \log q_2$ . Therefore by Proposition 25 we have

$$\mathcal{P}_\Omega^{(l)}(V_{q_1, q_2}(\gamma_1, \gamma_2)) \leq \mathcal{P}_\Omega^{(l)}(V(f_{g, \gamma_2})) \ll q_2^{-O_\Omega(1)}.$$

$\square$

*Proof of Proposition 53.* We have that

$$(45) \quad \mathcal{P}_\Omega^{(l)}(W_{a,q}) = \pi_q[\mathcal{P}_\Omega^{(l)}](\overline{W}_{a,q}) = \sum_{\overline{\gamma} \in \pi_q(\Gamma)} (\pi_q[\mathcal{P}_\Omega]^{(l-l_0)}(\overline{\gamma})) (\pi_q[\mathcal{P}_\Omega]^{(l_0)}(\overline{\gamma}^{-1} \overline{W}_{a,q}))$$

$$(46) \quad \leq \max_{\overline{\gamma} \in \pi_q(\Gamma)} \pi_q[\mathcal{P}_\Omega]^{(l_0)}(\overline{\gamma}^{-1} \overline{W}_{a,q})$$

if  $l_0 \leq l$ . So it is enough to prove

$$(47) \quad \mathcal{P}_\Omega^{(l_0)}(\gamma^{-1} W_{a,q}) \leq Q^{-O_\Omega(\varepsilon)}$$

for  $\varepsilon \log Q \ll l_0 \ll \varepsilon \log Q$ .

Since  $\gamma^{-1}W_{a,q} \cap \text{supp}(\mathcal{P}^{(l_0)}) \subseteq V_{q, \lfloor Q^{O_\Omega(\varepsilon)} \rfloor}(\gamma, a)$ , Corollary 55 implies the desired result.  $\square$

**4.6. Finding a torus with lots of  $p$ -adically large elements in  $A.A$ .** For the rest of this section, let  $\Omega$  and  $\Gamma$  be as in Section 2.6, and  $\mathcal{G}_1$ ,  $\mathcal{G}_{1,\mathfrak{p}}$ , and  $\pi_{p^n}$  be as in Section 3.1. Let  $\mathfrak{p} \in V_f(k) \setminus S$  which divides  $p \in V_f(\mathbb{Q})$ . Let the quadruple of a group scheme  $\mathcal{H}$ , a number field  $k'$ , a place  $\nu \in V_f(k')$ , and a finite subset  $S'$  of  $V_f(k')$  be either  $(\mathcal{G}_1, \mathbb{Q}, p, S_0)$  if  $p \notin S_0$ , or  $(\mathcal{G}_{1,\mathfrak{p}}, k(\mathfrak{p}), \mathfrak{p}, S_{\mathfrak{p}})$  where  $S_{\mathfrak{p}}$  is the set of restrictions of  $S$  to  $k(\mathfrak{p})$  if  $p \in S_0$ . Notice that in either case we have  $k'_\nu = \mathbb{Q}_p$  and  $\Gamma \subseteq \mathcal{H}(\mathcal{O}_{k'}(S'))$ . Let  $\mathbb{H}$  be the generic fiber of  $\mathcal{H}$ . So  $\text{Ad}(\mathbb{H}) = \oplus_i \mathbb{H}_i$  where  $\mathbb{H}_i$  is a  $k'$ -simple  $k'$ -group, and  $\text{Lie}(\mathbb{H}) = \oplus_i \text{Lie}(\mathbb{H}_i)$ . Let  $\text{pr}_i$  be the projection either from  $\text{Ad}(\mathbb{H})$  onto  $\mathbb{H}_i$ , or from  $\text{Lie}(\mathbb{H})$  onto  $\text{Lie}(\mathbb{H}_i)$ .

The main goal of this section is to show Proposition 56.

**Proposition 56.** *In the above setting, suppose  $0 < \varepsilon_2 \ll_\Omega \varepsilon_1 \ll_\Omega 1$ . Let  $N$  be a positive integer such that  $1 \ll_\Omega N\varepsilon_2$ , and  $Q = p^N$ . Fix a simple factor  $\mathbb{H}' := \mathbb{H}_{i_0}$  and let  $\text{pr} := \text{pr}_{i_0}$ . Then there are a positive real number  $\delta$ , positive integers  $n_1 = \Theta_{\Omega, i_0}(\varepsilon_1 N)$  (level) and  $n_2 = \Theta_{\Omega, i_0}(\varepsilon_1 N)$  (thickness) where the following holds:*

*Let  $n_3 = \Theta_{\Omega, i_0}(\varepsilon_2 N)$  (auxiliary number to get a  $p^{-n_3}$ -regular semisimple element). If  $\mathfrak{P}_Q(\delta, A, l)$  holds, then there are a maximal  $k'$ -torus  $\mathbb{T}$  of  $\mathbb{H}$  and  $\mathfrak{b} \subseteq \text{Lie}(\mathcal{H})(\mathbb{Z}_p) \cap \text{Lie}(\mathbb{T})(k')$  such that*

- (1)  $\pi_{p^{n_2}}(\text{pr}(\mathfrak{b})) \subseteq \Psi_{p^{n_1}}^{p^{n_1+n_2}}(\pi_{p^{n_1+n_2}}(\text{pr}(\prod_8 A)) \cap \pi_{p^{n_1+n_2}}(\Gamma[p^{n_1}]))$ ,
- (2)  $Q^{\Theta_\Omega(\varepsilon_1)} \leq |\text{pr}(\mathfrak{b})| = |\text{pr}(\pi_{p^{n_2}}(\mathfrak{b}))|$ ,
- (3) For any  $0 \leq m \leq n_2$ ,  $p^{\Theta_\Omega(m)} \leq |\text{pr}(\pi_{p^m}(\mathfrak{b}))|$ .

*Moreover there is a Galois extension  $k''$  of  $k'$  of degree at most  $n!$  such that  $\mathbb{T}$  splits over  $k''$  and for any  $\nu' \in V_f(k'')$  that divides  $\nu$  there are  $x_\phi \in \mathfrak{h}(\mathcal{O}_{\nu'}) \cap \mathfrak{h}_\phi((k'')_{\nu'})$  such that*

- (1)  $\mathcal{O}_{\nu'} x_\phi = \mathfrak{g}(\mathcal{O}_{\nu'}^{(i)}) \cap \mathfrak{g}_\phi(k''_{\nu'})$ ,
- (2)  $p^{n_3} \mathfrak{h}(\mathcal{O}_{\nu'}) \subseteq (\mathfrak{h}(\mathcal{O}_{\nu'}) \cap \mathfrak{t}(k''_{\nu'})) \oplus \bigoplus_{\phi \in \Phi(\mathbb{H}, \mathbb{T})} \mathcal{O}_{\nu'} x_\phi$ ,

*where  $\mathcal{O}_{\nu'}$  is the ring of integers of  $k''_{\nu'}$ .*

To this end, first we find a  $q^{-1}$ -regular semisimple element with *small*  $q$  and *large* centralizer in Proposition 58.

**Lemma 57.** *In the above setting, suppose  $0 < \delta \ll \varepsilon \ll 1$  and  $n, N$  are positive integers such that  $1 \ll_\Omega N\varepsilon \ll_\Omega n$ . Let  $Q := p^N$  and  $q := p^n$ . Also assume that  $\mathfrak{P}_Q(\delta, A, l)$  holds and  $\{a_i\}_{i=1}^{O_\Omega(1)} \subseteq \prod_{O_\Omega(1)} A$  is as in Proposition 44. Then*

$$\mathcal{P}_\Omega^{(2l_0)}(A.A \setminus \bigcup_{i=1}^{O_\Omega(1)} W_{a_i, q}) \geq Q^{-2\delta}/2,$$

*for any  $\varepsilon \log Q \ll_\Omega l_0 \leq l$ .*

*Proof.* Since  $\mathcal{P}_\Omega^{(l)}(A) \geq Q^{-\delta}$ , by Lemma 6 we have  $\mathcal{P}_\Omega^{(2l_0)}(A.A) \geq Q^{-2\delta}$ . Hence by Proposition 53, for  $\delta \ll_\Omega \varepsilon$  and  $1 \ll_\Omega Q^\varepsilon$  we have

$$\mathcal{P}_\Omega^{(2l_0)}(A.A \setminus \bigcup_{i=1}^{O_\Omega(1)} W_{a_i, q}) \geq Q^{-2\delta} - O_\Omega(1)Q^{-O_\Omega(\varepsilon)} \geq Q^{-2\delta}/2.$$

$\square$

**Proposition 58.** *In the above setting, suppose  $0 < \varepsilon_2 \ll_\Omega \varepsilon_1 \ll_\Omega 1$  and  $N$  is a positive integer such that  $1 \ll_\Omega \varepsilon_2 N$ . Let  $Q := p^N$ . Then there is a positive real number  $\delta$  where the following holds:*

*Let  $q_1 = p^{m_1}$  and  $q_2 = p^{m_1+m_2}$  such that  $m_1 = \Theta_\Omega(\varepsilon_1 N)$  and  $m_2 = \Theta_\Omega(\varepsilon_2 N)$ . If  $\mathfrak{P}_Q(\delta, A, l)$  holds, then there is  $x \in \prod_{O_\Omega, \varepsilon_1(1)} A$  such that*



- (1)  $x$  is  $|p^{m_2}|_\nu$ -regular semisimple.
- (2)  $|C_{\pi_{q_2}(\Gamma)}(\pi_{q_2}(x)) \cap \pi_{q_2}(A.A)| \geq Q^{\Theta_\Omega(\varepsilon_1)}$ .

*Proof.* We can and will assume that  $\delta \ll_\Omega \varepsilon_2$  and so there is  $\{a_i\}_{i=1}^{O_\Omega(1)} \subseteq \prod_{O_\Omega(1)} A$  as in Proposition 44. Let  $X = (A.A \setminus \bigcup_i W_{a_i, p^{m_2}}) \cap B_{2^{\lceil \varepsilon_1 \log Q \rceil}}$ . Now we know the following properties of  $X$ :

- (1) By Lemma 57 we have  $\mathcal{P}_\Omega^{(2^{\lceil \varepsilon_1 \log Q \rceil})}(X) \geq Q^{-2\delta}/2$ . So by the Kesten bound we have  $|X| \geq Q^{\Theta_\Omega(\varepsilon_1)}$ .
- (2) The  $S$ -norm of any element of  $X$  is at most  $Q^{\Theta_\Omega(\varepsilon_1)}$ . So  $|\pi_{q'}(X)| = |X|$  if  $\log q' \gg \varepsilon_1 \log Q$ .
- (3) By Lemma 46, for some  $x' \in X$ , some index  $i$ , and some  $q' \geq q_2 Q^{-\varepsilon_1}$ , we have that

$$|C_{\pi_{q_2}(\Gamma)}(\pi_{q_2}(x'a_i)) \cap \pi_{q_2}(A.A)| \geq |\pi_Q(A)|^{-\Theta_\Omega, \varepsilon_1(\delta)} |\pi_{q'}(X)|^{\Theta_\Omega(1)}.$$

Hence if we choose  $\delta$  small enough depending on  $\varepsilon_1$  and  $\varepsilon_2$ , then we have

$$|C_{\pi_{q_2}(\Gamma)}(\pi_{q_2}(x'a_i)) \cap \pi_{q_2}(A.A)| \geq Q^{\Theta_\Omega(\varepsilon_1)},$$

for some  $x' \in X$ . Since  $x' \in X$ ,  $x'a_i$  is a  $|p^{m_2}|_\nu$ -regular semisimple element.  $\square$

**Lemma 59** (Going to  $k'$ -simple factors). *In the above setting, if  $\mathfrak{P}_Q(\delta, A, l)$  holds for a positive integer  $Q$  and  $1 \gg_\Omega \delta > 0$ , then  $\mathfrak{P}_Q(\Theta_\Omega(\delta), \text{pr}_i(\text{Ad}(A \cdot A)), l)$  holds for any  $i$ .*

*Proof.* As it was discussed in Section 2.4,  $R_{k(\mathfrak{p})/\mathbb{Q}}(\mathbb{G}_{1,\mathfrak{p}})$  is naturally isomorphic to  $\mathbb{G}_1$ . And so, if  $\mathbb{G}'$  is a  $k(\mathfrak{p})$ -simple factor of  $\text{Ad}(\mathbb{G}_{1,\mathfrak{p}})$ , then  $R_{k(\mathfrak{p})/\mathbb{Q}}(\mathbb{G}')$  is naturally isomorphic to a  $\mathbb{Q}$ -simple factor of  $\mathbb{G}_1$ . Therefore, by Proposition 18, we have that the  $\text{pr}'(\text{Ad}(\overline{\Omega}))$  freely generates a Zariski-dense subgroup of  $R_{k(\mathfrak{p})/\mathbb{Q}}(\mathbb{G}')(\mathbb{Q})$ . Thus  $\text{pr}(\text{Ad}(\overline{\Omega}))$  freely generates a Zariski-dense subgroup of  $\mathbb{G}'(k(\mathfrak{p}))$ . Hence, for any index  $i$ ,  $\overline{\Omega}_i := \text{pr}_i(\text{Ad}(\overline{\Omega}))$  freely generates a Zariski-dense subgroup of  $\mathbb{H}_i(k')$ . Let  $\Omega_i := \overline{\Omega}_i \cup \overline{\Omega}_i^{-1}$ . Since  $\mathcal{P}_\Omega^{(l)}(A) \geq Q^{-\delta}$  and the restriction of  $\text{pr}_i \circ \text{Ad}$  to  $\Gamma$  is one-to-one, we have  $\mathcal{P}_{\Omega_i}^{(l)}(A_i) \geq Q^{-\delta}$ . So by Lemma 6 we have that  $\mathcal{P}_{\Omega_i}^{([\Theta_\Omega(\log Q)])}(A_i \cdot A_i) \geq Q^{-2\delta}$ . Hence by the Kesten bound we have  $|A_i \cdot A_i \cap B_{[\Theta_\Omega(\log Q)]}| \geq Q^{\Theta_\Omega(1)-2\delta} \geq Q^{\Theta_\Omega(1)}$ . For a suitable (implied) constant we have also  $|A_i \cdot A_i \cap B_{[\Theta_\Omega(\log Q)]}| = |\pi_Q(A_i \cdot A_i \cap B_{[\Theta_\Omega(\log Q)]})|$ . Thus overall we have that

- (1)  $\mathcal{P}_{\Omega_i}^{(l)}(A_i) \geq Q^{-\delta}$ , and
- (2)  $|\pi_Q(A_i \cdot A_i)| \geq Q^{\Theta_\Omega(1)} \geq |\pi_Q(A)|^{\Theta_\Omega(1)}$ .

Hence by the Rusza inequality we have that  $|\pi_Q(\prod_3(A_i \cdot A_i))| \leq |\pi_Q(A_i \cdot A_i)|^{1+\Theta_\Omega(\delta)}$ , which implies that  $\mathfrak{P}_Q(\Theta_\Omega(\delta), A_i \cdot A_i, l)$  holds for any  $i$ .  $\square$

*Proof of Proposition 56.* By Lemma 59 and the virtue of the proof of Proposition 58, we have that there is  $x_i \in \prod_{O_\Omega, \varepsilon_2(1)} A$  such that

- (1)  $x_i$  is  $|p^{n_3}|_\nu$ -regular semisimple.
- (2)  $|C_{\pi_{q'_2}(\rho_i(\Gamma))}(\pi_{q'_2}(\rho_i(x_i))) \cap \pi_{q'_2}(\rho_i(\prod_2(A.A)))| \geq Q^{\Theta_\Omega(\varepsilon_1)}$ , where  $\rho_i = \text{pr}_i \circ \text{Ad}$  and  $q'_2 = Q^{\Theta_\Omega(\varepsilon_1)}$ .

Using the  $p$ -adic topology on  $\rho_i(\Gamma)$  we can view  $\pi_{q'_2}(\rho_i(\Gamma))$  as a subset of a rooted regular tree  $T_{|f_\nu|^{\dim \mathbb{H}}, \log_p q'_2}$ . Hence by regularization, see Corollary 11, there are a positive integer  $n_1 = \Theta_\Omega(\varepsilon_1 N)$  and

$$\overline{B}_i \subseteq C_{\pi_{q'_2}(\rho_i(\Gamma))}(\pi_{q'_2}(\rho_i(x_i))) \cap \pi_{q'_2}(\rho_i(\prod_2(A.A)))$$

such that  $|\pi_{p^{n_1}}(\overline{B}_i)| = 1$  and  $|\pi_{p^l}(\overline{B}_i)| \gg_\Omega p^{\Theta_\Omega(l-n_1)}$  for any  $n_1 \leq l \leq \log_p q'_2$ ; in particular  $|\overline{B}_i| \gg Q^{\Theta_\Omega(\varepsilon_1)}$ .

Since  $x_i$  is  $|p^{n_3}|_\nu$ -regular semisimple,  $\rho_i(x_i)$  is also  $|p^{n_3}|_\nu$ -regular semisimple. Now, let's apply Lemma 52 to  $q_0 := p^{n_3}$ ,  $q := p^{n_3}$ ,  $q_1 := p^{n_1}$ , and  $q_2 := p^{n_1+n_2}$  where

$$n_2 := \min\{n_1 - 4n_3, \log_p q'_2 - n_1\}.$$

We notice that

$$\log_p q_0 = n_3 = \Theta_\Omega(N\varepsilon_2) \gg_\Omega 1,$$

and,

$$\log_p(q_1^2/(q_0 q^2 q_2)) = 2n_1 - (n_3 + 2n_3 + n_1 + n_2) \geq n_3 \gg_\Omega 1.$$

So the hypotheses of Lemma 52 hold. Therefore we have

$$\Psi_{q_1}^{q_2}(\pi_{q_2}(C_{\pi_{q_0 q^2 q_2}(\rho_i(\Gamma))}(\rho_i(x_i)) \cap \pi_{q_0 q^2 q_2}(\rho_i(\Gamma)[q_1]))) \subseteq \pi_{q_2/q_1}(\mathfrak{h}_i(\mathbb{Z}_p) \cap \bar{\mathfrak{t}}_i(k')),$$

where  $\bar{\mathfrak{t}}_i = \text{Lie } C_{\mathbb{H}_i}(\rho_i(x_i))$  and  $\mathfrak{h}_i := \text{Lie}(\mathcal{H}_i)$  where  $\mathcal{H}_i$  is the closure of  $\mathbb{H}_i$  in  $\mathcal{H}$ . Since  $|\pi_{q_1}(\bar{B}_i)| = 1$ ,  $\bar{B}_i \cdot \bar{B}_i^{-1} \subseteq \rho_i(\Gamma)[q_1]$ . Thus we have

$$\Psi_{q_1}^{q_2}(\pi_{q_2}(\bar{B}_i \cdot \bar{B}_i^{-1})) \subseteq \pi_{q_2/q_1}(\mathfrak{h}_i(\mathbb{Z}_p) \cap \bar{\mathfrak{t}}_i(k')).$$

On the other hand, since  $\rho_i(x_i)$  is a regular semisimple element, we have  $\text{pr}_i(\text{Lie } C_{\mathbb{H}}(x_i)) = \text{Lie } C_{\mathbb{H}_i}(\rho_i(x_i))$ . So we have

$$(48) \quad \Psi_{q_1}^{q_2}(\pi_{q_2}(\bar{B}_i \cdot \bar{B}_i^{-1})) \subseteq \pi_{q_2/q_1}(\mathfrak{h}_i(\mathbb{Z}_p) \cap \text{pr}_i(\mathfrak{t}_i(k'))),$$

where  $\mathfrak{t}_i := \text{Lie } C_{\mathbb{H}}(x_i)$ , and  $C_{\mathbb{H}}(x_i)^\circ$  is a  $k'$ -torus.

Since  $n_1 \leq n_1 + n_2 \leq \log_p q'_2$ , we have  $|\pi_{q_2}(\bar{B}_i)| \gg_\Omega p^{\Theta_\Omega(n_2)}$ . On the other hand, since  $n_1 = \Theta_\Omega(N\varepsilon_1)$  and  $\log_p q'_2 - n_1 = \Theta_\Omega(N\varepsilon_1)$ , we have

$$n_2 = \min\{\log_p q'_2 - n_1, n_1 - 4n_3\} = \Theta_\Omega(N\varepsilon_1)$$

if  $\varepsilon_2 \ll_\Omega \varepsilon_1$  for suitable constant.

The way we chose  $B_i$  implies that

- (1) For any  $q_1|q|q_2$  we have  $(q/q_1)^{\Theta_\Omega(1)} \ll_\Omega |\pi_q(\bar{B}_i \cdot \bar{B}_i^{-1})| = |\Psi_{q_1}^q(\pi_q(\bar{B}_i \cdot \bar{B}_i^{-1}))|$ .
- (2)  $Q^{\Theta_\Omega(\varepsilon_1)} \ll |\Psi_{q_1}^{q_2}(\pi_{q_2}(\bar{B}_i \cdot \bar{B}_i^{-1}))|$ .

Now one can find the desired  $k''$  and  $x_\phi$ 's by Lemma 51, Part (5). □

**4.7. Proof of Proposition 32.** As in the previous section, let  $\Omega$  and  $\Gamma$  be as in Section 2.6, and  $\mathcal{G}_1, \mathcal{G}_{1,\mathfrak{p}}$ , and  $\pi_{p^n}$  be as in Section 3.1. Let  $\mathfrak{p} \in V_f(k) \setminus S$  which divides  $p \in V_f(\mathbb{Q})$ . Let the quadruple of a group scheme  $\mathcal{H}$ , a number field  $k'$ , a place  $\nu \in V_f(k')$ , and a finite subset  $S'$  of  $V_f(k')$  be either  $(\mathcal{G}_1, \mathbb{Q}, p, S_0)$  if  $p \notin S_0$ , or  $(\mathcal{G}_{1,\mathfrak{p}}, k(\mathfrak{p}), \mathfrak{p}, S_\mathfrak{p})$  if  $p \in S_0$ . In particular,  $\Gamma \subseteq \mathcal{H}(\mathcal{O}_{k'}(S'))$ . Let  $\mathbb{H}$  be the generic fiber of  $\mathcal{H}$ . So  $\text{Ad}(\mathbb{H}) = \oplus_i \mathbb{H}_i$  where  $\mathbb{H}_i$  is a  $k'$ -simple  $k'$ -group, and  $\text{Lie}(\mathbb{H}) = \oplus_i \text{Lie}(\mathbb{H}_i)$ . Let  $\text{pr}_i$  be the projection either from  $\text{Ad}(\mathbb{H})$  onto  $\mathbb{H}_i$ , or from  $\text{Lie}(\mathbb{H})$  onto  $\text{Lie}(\mathbb{H}_i)$ .

For a given  $\varepsilon_1$  and  $\varepsilon_2$  (we consider  $\varepsilon_1$  and  $\varepsilon_2$  up to constants that depend only on  $\Omega$  and it will be clear what the conditions of the implied constants are), let  $\delta$  be the real number given by Proposition 56. We use Proposition 56 for any  $k'$ -simple factor  $\mathbb{H}_i$  of  $\text{Ad}(\mathbb{H})$ , and we get sets  $\mathfrak{b}_i$ , tori  $\mathbb{T}_i$ , finite Galois extensions  $k_i''$  of  $k'$ , divisors  $\nu_i'$  of  $\nu$ , and elements  $x_\phi^{(i)}$  that satisfy properties of Proposition 56. For simplicity let  $K_i := (k_i'')_{\nu_i'}$  and  $\mathcal{O}_i$  be the ring of integers of  $K_i$ . Let  $\Phi_i$  be the set of roots of  $\mathfrak{t}_i$  in  $d\rho_i = \text{pr}_i \circ \text{ad}$ . Let  $D : \mathfrak{t}_i(K_i) \rightarrow K_i^{|\Phi_i|}$ ,  $D(x) := (\phi(x))_{\phi \in \Phi_i}$ , and  $X_i := D(\mathfrak{b}_i) \subseteq \mathcal{O}_i^{|\Phi_i|}$ .

If  $D(b) \equiv D(b') \pmod{p^m \mathcal{O}_i^{|\Phi_i|}}$  for  $b, b' \in \mathfrak{b}_i$ , then  $\text{ad}(b)(x_\phi^{(i)}) \equiv \text{ad}(b')(x_\phi^{(i)}) \pmod{p^m \mathfrak{h}_i(\mathcal{O}_i)}$  for any  $\phi \in \Phi_i$ . So for any  $x \in \mathfrak{h}_i(\mathcal{O}_i)$  we have  $p^{n_3} \text{ad}(b)(x) \equiv p^{n_3} \text{ad}(b')(x) \pmod{p^m \mathfrak{h}_i(\mathcal{O}_i)}$ , where  $n_3$  is given by Proposition 56. Hence  $\pi_{p^{m'}}(b) = \pi_{p^{m'}}(b')$ , where  $m' = m - n_3 - \Theta_\Omega(1)$ . In particular,  $|\pi_{p^{n_2}}(X_i)| \geq Q^{\Theta_\Omega(\varepsilon_1)}$ , where  $n_2 \ll_\Omega n_2' \leq n_2$  and  $n_2 = \Theta_\Omega(\varepsilon_1 N)$  is given in Proposition 56. Hence by [SG-b, Theorem ?], there are integers  $m_1'$  and  $m_2' = \Theta_\Omega(\varepsilon_1 N)$  and  $\mathbf{d} \in \mathcal{O}_i^{|\Phi_i|} \setminus p\mathcal{O}_i^{|\Phi_i|}$  such that  $m_1' + m_2' \ll_\Omega n_2'$  and

$$\pi_{p^{m_1' + m_2'}}(p^{m_1'} \mathbb{Z} \mathbf{d}) \subseteq \pi_{p^{m_1' + m_2'}}(\sum_{O_\Omega(1)} \prod_{O_\Omega(1)} X_i - \sum_{O_\Omega(1)} \prod_{O_\Omega(1)} X_i).$$

Let  $\mathfrak{B}$  be a  $K_i$ -basis of which consists of  $\{x_\phi^{(i)}\}_{\phi \in \Phi_i}$  and a  $K_i$ -basis of  $\text{pr}_i(\mathfrak{t}_i(K_i))$ . For a linear map  $L$  in  $\text{End}_{K_i}(\mathfrak{h}_i(K_i))$ , let  $[L]_{\mathfrak{B}}$  be the corresponding matrix with respect to  $\mathfrak{B}$ . Therefore by enlarging  $n_3$  slightly we have:

$$\pi_{p^{m'_1+m'_2-n_3}}(p^{m'_1}\mathbb{Z} \text{diag}(\mathbf{d})) \subseteq \pi_{p^{m'_1+m'_2-n_3}}(\sum_{O_\Omega(1)} \prod_{O_\Omega(1)} [\text{ad}(\mathbf{b}_i)|_{\mathfrak{h}_i(K_i)}]_{\mathfrak{B}} - \sum_{O_\Omega(1)} \prod_{O_\Omega(1)} [\text{ad}(\mathbf{b}_i)|_{\mathfrak{h}_i(K_i)}]_{\mathfrak{B}}).$$

On the other hand, we know that  $\mathfrak{h}_i(K_i)$  has a basis  $\mathfrak{B}'$  such that

$$[\text{ad}(\mathbf{b}_i)|_{\mathfrak{h}_i(K_i)}]_{\mathfrak{B}'} \in M_{d_i}(\mathbb{Z}_p),$$

where  $d_i := \dim_{K_i}(\mathfrak{h}_i(K_i))$ . Hence there is  $b_i \in \text{End}_{\mathbb{Z}_p}(\mathfrak{h}_i(\mathbb{Z}_p)) \setminus p\text{End}_{\mathbb{Z}_p}(\mathfrak{h}_i(\mathbb{Z}_p))$  which is in the  $\mathbb{Q}_p$ -algebra generated by  $\text{ad}(\mathbf{b}_i)|_{\mathfrak{h}_i(K_i)}$  such that

$$(49) \quad \pi_{p^{m_1+m_2}}(p^{m_1}\mathbb{Z}_p b_i) \subseteq \pi_{p^{m_1+m_2}}(\sum_{O_\Omega(1)} \prod_{O_\Omega(1)} d\rho_i(\mathbf{b}_i) - \sum_{O_\Omega(1)} \prod_{O_\Omega(1)} d\rho_i(\mathbf{b}_i)).$$

Since  $b_i$  is in the  $\mathbb{Q}_p$ -algebra generated by  $\text{ad}(\mathbf{b}_i)|_{\mathfrak{h}_i(K_i)}$ , we have that  $b_i(x_\phi^{(i)}) = b_{i,\phi}x_\phi^{(i)}$  for any  $\phi \in \Phi_i$ .

Now without loss of generality we can and will assume that  $m_1 + m_2 = n_2$ .

**Lemma 60.** *If  $t_j \equiv 1 + p^m y_j \pmod{p^{2m}}$  for  $1 \leq j \leq N$ ,  $\gamma_0 \equiv 1 + p^k \xi_0 \pmod{p^{2k}}$  and  $k \geq m$ , then*

$$C_{t_1} \circ C_{t_2} \circ \cdots \circ C_{t_N}(\gamma_0) \equiv 1 + p^{k+Nm} \text{ad}(y_1) \text{ad}(y_2) \cdots \text{ad}(y_N) \xi_0 \pmod{p^{k+(N+1)m}},$$

where  $C_t(\gamma) := t\gamma t^{-1}\gamma^{-1}$ .

*Proof.* We proceed by induction on  $N$ . For  $N = 1$ , we have

$$\begin{aligned} C_t(\gamma) &\equiv 1 + [t, \gamma] \pmod{p^{m+k+\min\{m,k\}}} \\ &\equiv 1 + ((1 + p^m y')(1 + p^k \xi') - (1 + p^k \xi')(1 + p^m y')) \pmod{p^{2m+k}} \\ &\equiv 1 + p^{m+k} [y', \xi'] \pmod{p^{2m+k}} \\ &\equiv 1 + p^{m+k} [y, \xi] \pmod{p^{2m+k}} \quad (\text{since } y' \equiv y \pmod{p^m}, \xi' \equiv \xi \pmod{p^k}). \\ &\equiv 1 + p^{m+k} \text{ad}(y) \xi \pmod{p^{2m+k}}. \end{aligned}$$

By a similar argument the inductive step can be proved.  $\square$

**Corollary 61** (Thick segment, conditional). *If  $\xi_0 \in \Psi_{p^k}^{2k}(\prod_{O_\Omega(1)} A)$  and  $k \geq n_2$ , where  $n_2 = \Theta(\varepsilon_1 N)$  is given in Proposition 56, then there are a positive integer  $m_1$  and  $b_i \in \text{End}_{\mathbb{Z}_p}(\mathfrak{h}_i(\mathbb{Z}_p)) \setminus p\text{End}_{\mathbb{Z}_p}(\mathfrak{h}_i(\mathbb{Z}_p))$  such that*

- (1)  $n_2 - m_1 = \Theta_\Omega(\varepsilon_1 N)$ ,
- (2)  $\pi_{p^{n_2}}(p^{m_1}\mathbb{Z}_p b_i(\text{pr}_i(\xi_0))) \subseteq \text{pr}_i\left(\Psi_{p^{k+n'_1}}^{p^{k+n'_1+n_2}}(\prod_{O_\Omega(1)} A \cap \Gamma[p^{k+n'_1}])\right)$ , where  $n'_1 = \Theta_\Omega(n_1)$  and  $n_1$  is given in Proposition 56.

*Proof.* By Proposition 56, we have

$$\pi_{p^{n_1+n_2}}(1 + p^{n_1} \mathbf{b}_i) \subseteq \pi_{p^{n_1+n_2}}(\prod_{O_\Omega(1)} A).$$

Hence by Lemma 60 we have that

$$(50) \quad \pi_{p^{k+n'_1+n_2}}\left(1 + p^{k+n'_1}\left(\sum_{O_\Omega(1)} \prod_{O_\Omega(1)} \text{ad}(\mathbf{b}_i) - \sum_{O_\Omega(1)} \prod_{O_\Omega(1)} \text{ad}(\mathbf{b}_i)\right)(\xi_0)\right) \subseteq \pi_{p^{k+n'_1+n_2}}(\prod_{O_\Omega(1)} A),$$

where  $n'_1 = \Theta_\Omega(n_1)$ . Now one can complete the proof using (49).  $\square$

Corollary 61 gives us a *thick segment* only when  $b_i(\text{pr}_i(\xi_0))$  has a large  $p$ -adic norm, which happens if  $\xi_0$  is away from  $\bigcup_{\phi \in \Phi_i} W_\phi$  where  $W_\phi := \mathfrak{t}_i \oplus \bigoplus_{\phi' \neq \phi} \mathfrak{g}_{\phi'}$ .

**Lemma 62** (Thick segment). *Let  $n_1 = \Theta_\Omega(N\varepsilon_1)$  and  $n_2 = \Theta_\Omega(N\varepsilon_1)$  be as in Proposition 56. There are integers  $m_1$  and  $n_1'' = \Theta_\Omega(n_1)$  and  $\xi_0 \in \mathfrak{h}_i(\mathbb{Z}_p) \setminus p\mathfrak{h}_i(\mathbb{Z}_p)$  such that  $n_2 - m_1 = \Theta_\Omega(N\varepsilon_1)$  and*

$$\pi_{p^{n_2}}(p^{m_1}\mathbb{Z}_p\xi_0) \subseteq \text{pr}_i \left( \Psi_{p^{n_1''}}^{p^{n_1''}+n_2} (\prod_{O_\Omega(1)} A \cap \Gamma[p^{n_1'}]) \right).$$

*Proof.* Applying Proposition 40 for  $\varepsilon := \varepsilon_2$ , representation  $\rho := \rho_i$ , number field  $k'$ , and  $S'$ , we get  $\{a_j\}_{j=1}^{O_\Omega(1)} \subseteq \prod_{O_\Omega(1)} A$  such that

$$(51) \quad [\mathbb{Z}_p[\rho_i(\Gamma)] : \sum_j \mathbb{Z}_p \rho_i(a_j)] \leq Q^{\varepsilon_2}.$$

On the other hand,  $\mathfrak{h}_i(k')$  is a simple  $\rho_i(\Gamma)$ -module, and  $k'_\nu = \mathbb{Q}_p$ . Hence for any  $x \in \mathfrak{h}_i(\mathbb{Q}_p) \setminus \{0\}$  we have

$$(52) \quad \mathfrak{h}_i(\mathbb{Q}_p) = \mathbb{Q}_p[\rho_i(\Gamma)](x).$$

Moreover for large enough  $p$  we have  $\mathbb{Z}_p[\rho_i(\Gamma)]$  is a maximal order of the central simple algebra  $\mathbb{Q}_p[\rho_i(\Gamma)]$ . Thus for large enough  $p$  and  $x \in \mathfrak{h}_i(\mathbb{Z}_p) \setminus p\mathfrak{h}_i(\mathbb{Z}_p)$  we have  $\mathfrak{h}_i(\mathbb{Z}_p) = \mathbb{Z}_p[\rho_i(\Gamma)](x)$ . For arbitrary  $p$ , by a compactness argument similar to [SG05, Lemma 3.5], we have that  $[\mathfrak{h}_i(\mathbb{Z}_p) : \mathbb{Z}_p[\rho_i(\Gamma)](x)] \ll_\Omega 1$  for  $x \in \mathfrak{h}_i(\mathbb{Z}_p) \setminus p\mathfrak{h}_i(\mathbb{Z}_p)$ . Hence, by (51) and (52), for  $x \in \mathfrak{h}_i(\mathbb{Z}_p) \setminus p\mathfrak{h}_i(\mathbb{Z}_p)$ , we have

$$(53) \quad [\mathfrak{h}(\mathbb{Z}_p) : \sum_j \mathbb{Z}_p \rho_i(a_j)(x)] = [\mathfrak{h}(\mathbb{Z}_p) : \mathbb{Z}_p[\rho_i(\Gamma)](x)] [\mathbb{Z}_p[\rho_i(\Gamma)](x) : \sum_j \mathbb{Z}_p \rho_i(a_j)(x)] \ll_\Omega Q^{\varepsilon_2}.$$

**Claim.** We have  $\max_j \|b_i(\rho_i(a_j)(x))\|_p \geq Q^{-\Theta_\Omega(\varepsilon_2)}$  for any  $x \in \mathfrak{h}_i(\mathbb{Z}_p) \setminus p\mathfrak{h}_i(\mathbb{Z}_p)$ .

*Proof of Claim.* Suppose  $\max_j \|b_i(\rho_i(a_j)(x))\|_p = |q|_p$  where  $q$  is a power of  $p$ . So for any  $j$  we have  $b_i(\rho_i(a_j)(x)) \in q\mathfrak{h}_i(\mathbb{Z}_p)$ . Hence

$$(54) \quad \sum_j \mathbb{Z}_p b_i(\rho_i(a_j)(x)) \subseteq q\mathfrak{h}_i(\mathbb{Z}_p).$$

Therefore by (53) and (54) we have

$$p^{\Theta_\Omega(n\varepsilon_2)} \mathfrak{h}_i(\mathbb{Z}_p) \subseteq \sum_j \mathbb{Z}_p b_i(\rho_i(a_j)(x)) \subseteq q\mathfrak{h}_i(\mathbb{Z}_p),$$

which implies that  $q \leq Q^{\Theta_\Omega(\varepsilon_2)}$ , and it gives us the claim.

By the easy part of the proof of Proposition 56, there are  $x \in \mathfrak{h}_i(\mathbb{Z}_p) \setminus p\mathfrak{h}_i(\mathbb{Z}_p)$  and  $\gamma \in \prod_8 A \cap \Gamma[p^k]$  such that  $\pi_{p^k}(x) = \Psi_{p^k}^{p^{2k}}(\gamma)$  and  $n_1 \leq k < 2n_1$ . Therefore by Lemma 29 and Proposition 40 we have

$$\pi_{p^{2k}}(\rho_i(a_j)(x)) \in \text{pr}_i \left( \Psi_{p^k}^{p^{2k}} \left( \prod_{O_\Omega(1)} A \cap \Gamma[p^k] \right) \right),$$

for any  $i, j$ , and  $\rho_i(a_j)(x) \in \mathfrak{h}_i(\mathbb{Z}_p) \setminus p\mathfrak{h}_i(\mathbb{Z}_p)$ . Hence by Corollary 61 we have

$$\pi_{p^{n_2}}(p^{m_1}\mathbb{Z}_p b_i(\rho_i(a_j)(x))) \subseteq \text{pr}_i \left( \Psi_{p^{n_1'}}^{p^{n_1'}+n_2} \left( \prod_{O_\Omega(1)} A \cap \Gamma[p^{n_1'}] \right) \right),$$

where  $n_1' = \Theta_\Omega(n_1)$  and  $n_2 - m_1 = \Theta_\Omega(\varepsilon_1 N)$ . Thus by the above claim for some  $j$  we have  $b_i(\rho_i(a_j)(x)) = p^{m_1'} \xi_0$  for some  $\xi_0 \in \mathfrak{h}_i(\mathbb{Z}_p) \setminus p\mathfrak{h}_i(\mathbb{Z}_p)$  and  $m_1' \ll_\Omega \varepsilon_2 N$ . Since  $n_2 - m_1 - m_1' = \Theta_\Omega(\varepsilon_1 N) - \Theta_\Omega(\varepsilon_2 N)$ , for a suitable choice of the implied constant in  $\varepsilon_2 \ll_\Omega \varepsilon_1$  we have  $n_2 - m_1 - m_1' = \Theta_\Omega(\varepsilon_1 N)$ . This completes the proof.  $\square$

**Lemma 63** (Thick top slice: simple factors). *For any  $i$  there are positive integers  $n_1^{(i)}$  (level) and  $n_2^{(i)}$  (thickness) such that*

$$(1) \quad n_1^{(i)} = \Theta_\Omega(\varepsilon_1 n) \text{ and } n_2^{(i)} = \Theta_\Omega(\varepsilon_1 n).$$

$$(2) \quad \pi_{p^{n_2}^{(i)}}(\mathfrak{h}_i(\mathbb{Z}_p)) \subseteq \text{pr}_i \left( \Psi_{p^{n_1}^{(i)}}^{p^{n_1}^{(i)} + n_2^{(i)}} (\prod_{O_\Omega(1)} A \cap \Gamma[p^{n_1}^{(i)}]) \right).$$

*Proof.* Without loss of generality, we fix  $i$ . Let  $\{a_j\}_{j=1}^{O_\Omega(1)} \subseteq \prod_{O_\Omega, \varepsilon_2(1)} A$  be as in Proposition 40 and  $\xi_0 \in \mathfrak{h}_i(\mathbb{Z}_p) \setminus p\mathfrak{h}_i(\mathbb{Z}_p)$  be as in Lemma 62. Then after changing  $\varepsilon_2$  by a constant which just depends on  $\Omega$  we have  $|\mathfrak{h}_i(\mathbb{Z}_p)/\sum_j \mathbb{Z}_p \rho_i(a_j)(\xi_0)| \leq Q^{\varepsilon_2}$ . Hence for some positive integer  $m = \Theta_\Omega(\varepsilon_2 n)$  we have  $p^m \mathfrak{h}_i(\mathbb{Z}_p) \subseteq \sum_j \mathbb{Z}_p \rho_i(a_j)(\xi_0)$ . Therefore by Lemma 62

$$\pi_{p^{n_2}}(p^{m_1+m} \mathfrak{h}_i(\mathbb{Z}_p)) \subseteq \text{pr}_i \left( \Psi_{p^{n_1}''}^{p^{n_1}'' + n_2} (\prod_{O_\Omega(1)} A \cap \Gamma[p^{n_1}'']) \right),$$

where  $n_2 = \Theta_\Omega(\varepsilon_1 n)$ ,  $n_1'' = \Theta_\Omega(\varepsilon_1 n)$ ,  $m_1$  are as in Lemma 62. Notice that  $n_2 - m_1 - m = \Theta_\Omega(\varepsilon_1 n) - \Theta_\Omega(\varepsilon_2 n)$  and so  $n_2 - m_1 - m = \Theta_\Omega(\varepsilon_1 n)$  as  $\varepsilon_2 \ll_\Omega \varepsilon_1$ .  $\square$

Inspired by Definition 36, let us say  $\mathcal{B}_i(L, T)$  holds if for some  $q_1 | q_2 | q_1^2$  that are powers of  $p$  we have

$$\pi_{q_2}(\mathfrak{h}_i(\mathbb{Z}_p)) \subseteq \Psi_{q_2}^{q_1} (\prod_{O_\Omega, \varepsilon_1, \varepsilon_2(1)} A \cap \Gamma[q_1]),$$

and  $q_1 \leq L$  and  $LT \leq q_2$ . By the virtue of proofs of Lemma 37 and Corollary 38, we have that

**Lemma 64.** *There is a constant  $q_0$  depending only on  $\Omega$  such that if  $\mathcal{B}_i(L, T)$  and  $\mathcal{B}_i(L', T')$  hold,  $L, L' \geq T$ ,  $L, L' \gg_\Omega 1$  and  $\log T' = \Theta_\Omega(\log T)$ , then  $\mathcal{B}_i(q_0 LL', TT'/q_0)$  holds.*

**Lemma 65** (Leveling top slices). *There are positive integers  $n_1$  and  $n_2$  such that*

- (1)  $n_1 = \Theta_\Omega(\varepsilon_1 n)$  and  $n_2 = \Theta_\Omega(\varepsilon_1 n)$ .
- (2)  $\pi_{p^{n_2}}(\mathfrak{h}_i(\mathbb{Z}_p)) \subseteq \text{pr}_i \left( \Psi_{p^{n_1}}^{p^{n_1} + n_2} (\prod_{O_\Omega(1)} A \cap \Gamma[p^{n_1}]) \right)$  for any  $i$ .

*In particular, we have  $\pi_{p^{n_2}}(\mathfrak{h}(\mathbb{Z}_p)) \subseteq \Psi_{p^{n_1}}^{p^{n_1} + n_2} (\prod_{O_\Omega(1)} A \cap \Gamma[p^{n_1}])$ .*

*Proof.* By Lemma 63, we know that  $\mathcal{B}_i(p^{n_1}^{(i)}, p^{n_2}^{(i)})$  holds for any  $i$ , for some integers  $n_1^{(i)} = \Theta_\Omega(\varepsilon_1 n)$  and  $n_2^{(i)} = \Theta_\Omega(\varepsilon_1 n)$ . Hence by repeated use of Lemma 64 we have that  $\mathcal{B}_i(p^{ln_1^{(i)} + ln_0}, p^{ln_2^{(i)} - ln_0})$  holds for any  $l = O_\Omega(1)$  and any  $i$ , where  $|q_0|_p = p^{-n_0}$ . Therefore, since  $[(n_1^{(i)} + n_0)/(n_2^{(i)} - n_0)]^2 = O_\Omega(1)$ , for any

$$\left\lceil \frac{n_1^{(i)} + n_0}{n_2^{(i)} - n_0} \right\rceil \leq l \leq \left\lceil \frac{n_1^{(i)} + n_0}{n_2^{(i)} - n_0} \right\rceil^2,$$

we have  $\mathcal{B}_i(p^{ln_1^{(i)} + ln_0}, p^{ln_2^{(i)} - ln_0})$  holds. These properties together imply that

$$\mathcal{B}_i(p^{l_0 n_1^{(i)} + l_0 n_0}, p^{l_0 n_1^{(i)} + l_0 n_0})$$

holds for  $l_0 = \lceil (n_1^{(i)} + n_0)/(n_2^{(i)} - n_0) \rceil = O_\Omega(1)$ . So without loss of generality we can and will assume that  $n_1^{(i)} = n_2^{(i)}$ .

For  $i \neq i'$ , we level the top thick layers of the  $i$ -th and the  $i'$ -th factors. Without loss of generality, let's assume that  $n_1^{(i)} \leq n_1^{(i')}$ . Since  $n_1^{(i)} = \Theta_\Omega(N\varepsilon_1)$  and  $n_1^{(i')} = \Theta_\Omega(N\varepsilon_1)$ , there is a positive integer  $l_0 \ll_\Omega 1$  such that  $n_1^{(i')} \leq 2^{l_0} n_1^{(i)}$ . Hence

$$(55) \quad [n_1^{(i')}, 2n_1^{(i')}] \subseteq \bigcup_{j=0}^{l_0-1} [2^j n_1^{(i)} + 2^{j-1} n_0, 2^{j+1} n_1^{(i)}] \cup \bigcup_{j=1}^{l_0-1} (2^j n_1^{(i)}, 2^j n_1^{(i)} + 2^{j-1} n_0).$$

Since  $N\varepsilon_1 \gg_\Omega 1$ ,  $n_1^{(i)} = \Theta_\Omega(N\varepsilon_1)$ , and  $l_0 \ll_\Omega 1$ , there is  $j$  such that

$$(56) \quad |[n_1^{(i')}, 2n_1^{(i')}] \cap [2^j n_1^{(i)} + 2^{j-1} n_0, 2^{j+1} n_1^{(i)}]| \gg_\Omega N\varepsilon_1.$$

On the other hand, by Lemma 64, for any integer  $0 \leq j \leq l_0 - 1$  we have that

$$\mathcal{B}_i(p^{2^j n_1^{(i)} + 2^{j-1} n_0}, p^{2^j n_1^{(i)} - 2^{j-1} n_0})$$

holds. Hence if  $[t_j, t_j + t'_j] := [n_1^{(i')}, 2n_1^{(i')}] \cap [2^j n_1^{(i)} + 2^{j-1} n_0, 2^{j+1} n_1^{(i)}]$ , then

$$\mathcal{B}_i(p^{t_j}, p^{t'_j}), \text{ and } \mathcal{B}_{i'}(p^{t_j}, p^{t'_j})$$

hold. By (56) for some  $j$  the above closed interval  $[t_j, t_j + t'_j]$  is thick enough, and works for both the  $i$ -th and the  $i'$ -th factors. Now by induction on the number of simple factors, we can find  $n_1$  and  $n_2$  that work for all the simple factors at the same time. And therefore we get

$$\pi_{p^{n_2}}(\mathfrak{h}(\mathbb{Z}_p)) \subseteq \Psi_{p^{n_1}}^{p^{n_1+n_2}}(\prod_{O_\Omega(1)} A \cap \Gamma[p^{n_1}]).$$

□

Lemma 65 and Lemma 29 imply Proposition 32.

## 5. APPENDIX A: A SMALL SOLUTION.

**5.1. Logarithmic height, and the statement of the main result.** In this appendix, we recall the (logarithmic and multiplicative) height of a point and prove that any closed subscheme of  $(\mathbb{A}_n)_{\mathbb{Q}}$  with a closed geometric point has a *small* closed geometric point.

For any prime  $p$ , a place  $|\cdot|_p$  on  $\mathbb{Q}$  is fixed such that  $|p|_p = 1/p$ . If  $k$  is a Galois number field, then a place  $\mathfrak{p}|p$  is normalized such that  $|x|_{\mathfrak{p}} := |N_{k/\mathbb{Q}}(x)|_p^{1/[k:\mathbb{Q}]}$  and in particular for any  $x \in k$  we have the product formula  $\prod_{\mathfrak{p} \in \text{Pl}(k)} |x|_{\mathfrak{p}} = 1$  where  $\text{Pl}(k)$  is the set of inequivalence places of  $k$  (within the article the set of finite places is denoted by  $V_f(k)$ ). Let  $|x|_{\mathfrak{p}}^+ := \max\{1, |x|_{\mathfrak{p}}\}$ , and for a finite place let  $\|\mathbf{x}\|_{\mathfrak{p}} := \max_i \{|x_i|_{\mathfrak{p}}\}$  and  $\|\mathbf{x}\|_{\mathfrak{p}}^+ := \max_i \{|x_i|_{\mathfrak{p}}^+\}$ .

Any point  $v \in \mathbb{P}^n(\overline{\mathbb{Q}})$  can be represented by  $\mathbf{x} := (x_0, x_1, \dots, x_n) \in k^{n+1}$  where  $k$  is a Galois number field. We define the height  $h(v)$  of  $v$  to be

$$h(v) := \sum_{\mathfrak{p} \in \text{Pl}(k)} \log \|\mathbf{x}\|_{\mathfrak{p}}.$$

It is well-known that  $h(v)$  is independent of the choice of  $k$  and the choice of a representative (e.g. see [BG06, Chapter 1]). The height  $h(\mathbf{x})$  of  $\mathbf{x} = (x_1, \dots, x_n) \in \overline{\mathbb{Q}}^n$  is defined to be  $h(1:x_1:\dots:x_n) = \sum_{\mathfrak{p} \in \text{Pl}(k)} \log \|\mathbf{x}\|_{\mathfrak{p}}^+$ . The multiplicative height of a point  $\mathbf{x}$  in  $\mathbb{P}(\overline{\mathbb{Q}})$  or  $\mathbb{A}^n(\overline{\mathbb{Q}})$  is defined to be  $e^{h(\mathbf{x})}$ . Considering  $(\text{GL}_d)_{\mathbb{Q}}$  as an open subset of  $\text{End}_{\mathbb{Q}^d}$ , we can talk about the height  $h(X)$  of  $X \in \text{GL}_d(\overline{\mathbb{Q}})$ . The height  $h(f)$  of a polynomial  $f \in \mathbb{Q}[\underline{X}] = \mathbb{Q}[X_1, \dots, X_n]$  is defined to be

$$h(\sum_I a_I \underline{X}^I) := \sum_{\mathfrak{p} \in \text{Pl}(k)} \log(\max_I |a_I|_{\mathfrak{p}}),$$

where  $k$  is a Galois number field such that  $f \in k[\underline{X}]$  and  $\underline{X}^I = \prod_{i=1}^n X_i^{m_i}$  for  $I = (m_1, \dots, m_n)$ .

The main result of this appendix is the following Proposition.

**Proposition 66.** *Let  $k$  be a number field, and  $f_1, \dots, f_m \in k[X_1, \dots, X_n]$ . If there is  $\mathbf{x} \in \overline{\mathbb{Q}}^n$  such that  $f_1(\mathbf{x}) = \dots = f_m(\mathbf{x}) = 0$ , then there is  $\mathbf{x}_0 \in \overline{\mathbb{Q}}^n$  such that*

- (1)  $f_1(\mathbf{x}_0) = \dots = f_m(\mathbf{x}_0) = 0$ ,
- (2)  $h(\mathbf{x}_0) \ll \max_i h(f_i)$ , where the implied constant depends on  $n$ ,  $\max_i \deg f_i$ , and  $k$ .

**5.2. Reduction to the geometrically zero-dimensional case.** Let  $V = \text{Spec}(\mathbb{Q}[\underline{X}]/\langle f_1, \dots, f_m \rangle)$ . In this section, we reduce the dimension of  $V$  by proving that  $V$  intersects a hyperplane with *small* height. Providing such a process implies that it suffices to prove Proposition 66 under the additional assumption  $\dim V = 0$ .

**Lemma 67.** *Let  $V = \text{Spec}(\mathbb{Q}[\underline{X}]/\langle f_1, \dots, f_m \rangle)$ . If  $\dim V \geq 1$ , then there is  $\mathbf{x} \in \mathbb{Q}^n$  such that*

- (1)  $V(\overline{\mathbb{Q}}) \cap \ker(l_{\mathbf{x}})(\overline{\mathbb{Q}}) \neq \emptyset$ , where  $\ker(l_{\mathbf{x}})(\overline{\mathbb{Q}}) = \{\mathbf{y} \in \overline{\mathbb{Q}}^n \mid l_{\mathbf{x}}(\mathbf{y}) := \sum_i x_i y_i = 0\}$ ,
- (2)  $V(\overline{\mathbb{Q}}) \not\subseteq \ker(l_{\mathbf{x}})(\overline{\mathbb{Q}})$ ,
- (3)  $h(\mathbf{x}) \ll \max_i h(f_i)$ , where the implied constant depends on  $n$  and  $\max_i \deg f_i$ .

*Proof.* Let  $W(F) := \{[\mathbf{x}] \in \mathbb{P}^{n-1}(F) \mid V(\overline{\mathbb{Q}}) \cap \ker(l_{\mathbf{x}})(\overline{\mathbb{Q}}) = \emptyset\}$ , where  $F$  is a subfield of  $\overline{\mathbb{Q}}$ . By the nullstellensatz theorem,  $[\mathbf{x}] \in W(\mathbb{Q})$  if and only if there are  $q_0, q_i \in \mathbb{Q}[\underline{X}]$  such that

$$(57) \quad 1 = q_0(\underline{X})l_{\mathbf{x}}(\underline{X}) + \sum_i q_i(\underline{X})f_i(\underline{X}).$$

So by the effective Bezout (e.g. see [BY91]) we can assume further that

$$(58) \quad \max_i \deg(q_i) \ll 1,$$

and

$$(59) \quad \max_i h(q_i) \ll \max\{h([\mathbf{x}]), h(f_1), \dots, h(f_m)\},$$

where the implied constants depend on  $n$  and  $\max_j \deg f_j$ . By (58),  $q_i$  are in a finite-dimensional subspace of  $\mathbb{Q}[\underline{X}]$  and so the vector  $v_i$  of their coefficients is in a fixed finite-dimensional vector space. Comparing the coefficients of  $\underline{X}^I$  in the both sides of Equation (57), we get a system of equations

$$(60) \quad L_i(\mathbf{x}, v_j) = n_i,$$

where  $L_i$  are linear in  $\mathbf{x}$  and  $v_j$  for any  $j$ ,  $h(L_i) \ll \max_i h(f_i)$  where the implied constant depends on  $n$  and  $\max_i \deg(f_i)$ , and  $n_i$  are either 0 or 1 (they are zero except once). So  $[\mathbf{x}] \in W(F)$  if and only if Equation (60) has a solution with entries in  $F$ . Considering (60) as a system of linear equations over  $\mathbb{Q}[\underline{X}]$ , we get a (rectangular) matrix  $A$  with entries in  $\mathbb{Q}[\underline{X}]$  such that (60) has a solution if and only if  $A\mathbf{v} = \mathbf{e}_1$  has a solution, where all the components of  $\mathbf{e}_1$  are zero except the first one. It is well-known that there are invertible matrices  $P_1$  and  $P_2$  such that  $A = P_1 D P_2$  where the only non-zero entries of  $D$  are in the  $i, i$  position for some  $i$ . Let  $s(\underline{X})$  be the product of the denominators of the entries of  $P_1^{-1}$  and  $P_2$ . Thus, if  $s(\mathbf{x}) \neq 0$ , then (60) has a solution if and only if  $D(\mathbf{x})\mathbf{v} = P_1(\mathbf{x})^{-1}\mathbf{e}_1$  has a solution. And the latter happens if and only if  $r_1(\mathbf{x}) = \dots = r_c(\mathbf{x}) = 0$  for certain polynomials  $r_i(\underline{X}) \in \mathbb{Q}[\underline{X}]$ . Hence altogether there are polynomials  $s, r_i$  such that

$$(61) \quad W(F) \setminus \{[\mathbf{x}] \mid \mathbf{x} \in V(s)(F)\} = \{[\mathbf{x}] \mid \mathbf{x} \in V(r_1, \dots, r_c)(F) \setminus V(s)(F)\}.$$

Since  $\dim V > 1$ ,  $\dim W < n - 1$ . Hence in (61) we can assume that  $r_1$  is a non-zero homogeneous polynomial. It is also easy to see that the logarithmic height of the non-zero entries of  $P_1$ ,  $P_2$  and  $D$  are  $O(\max_i h(f_i))$  where the implied constant depends on the size of matrices (which is a function of the number of variables  $n$  and  $\max_i \deg f_i$ ) and their degree depends just on  $n$  and  $\max_i \deg f_i$ . Thus  $h(r_1) \ll \max_i h(f_i)$  where the implied constant depends only on  $n$  and  $\max_i \deg f_i$ . Now let  $p$  be a prime number such that  $\max_i h(f_i) \ll p \ll \max_i h(f_i)$ . Then

$$(62) \quad |\{[\mathbf{x}] \in W(\mathbb{Q}) \mid h([\mathbf{x}]) \leq p/2\}| \leq |\{[\mathbf{x}] \mid \mathbf{x} \in V(r_1)(\mathfrak{f}_p) \cup V(s)(\mathfrak{f}_p)\}| \ll p^{n-2}.$$

where the implied constant depends on the degrees of  $r_1$  and  $s$ . Hence choosing the constants correctly we can find a point  $[\mathbf{x}] \in \mathbb{P}^n(\mathbb{Q})$  such that

- (1)  $h([\mathbf{x}]) \ll \max_i h(f_i)$  where the implied constant depends only on  $n$  and  $\max_i \deg f_i$ .
- (2)  $[\mathbf{x}]$  is not in  $W(\mathbb{Q})$ , which means  $V(\overline{\mathbb{Q}}) \cap \ker(l_{\mathbf{x}})(\overline{\mathbb{Q}}) \neq \emptyset$ .

If  $V(\overline{\mathbb{Q}})$  is not a subset of  $\ker(l_{\mathbf{x}})(\overline{\mathbb{Q}})$ , we are done. If not, then we can repeat the above argument after taking a bases  $\mathbf{v}_1, \dots, \mathbf{v}_{n-1}$  for  $\ker l_{\mathbf{x}}$  such that  $h(\mathbf{v}_i) \ll \max_i h(f_i)$ , and rewriting all the functions in this coordinate systems. Now by a dimensional argument, in finitely many steps we get the desired  $\mathbf{x}$ .  $\square$

**5.3. Reduction to the complete intersection, geometrically zero-dimensional case.** By Lemma 67, Proposition 66 can be reduced to the (geometrically) zero-dimensional case. In this section, we make further reduction to the case of a complete intersection, geometrically zero-dimensional case. And then invoking the arithmetic Bézout theorem [BGS94, Theorem 5.5.1] Proposition 66 is proved.

**Lemma 68.** *Let  $V = \text{Spec}(\overline{\mathbb{Q}}[\underline{X}]/\langle f_1, \dots, f_m \rangle)$ . Suppose that  $\dim V = d$ . Then for  $1 \leq k \leq n - d$  there are  $\tilde{f}_1, \dots, \tilde{f}_k \in \overline{\mathbb{Q}}[\underline{X}]$*

- (1) *For any  $i$ ,  $\tilde{f}_i \in \mathbb{Z}f_1 + \mathbb{Z}f_2 + \dots + \mathbb{Z}f_m$ .*
- (2) *For any  $i$ ,  $h(\tilde{f}_i) \ll \max_j h(f_j)$  where the implied constant depends on  $n$  and the degree of  $f_j$ .*
- (3)  *$\dim(\overline{\mathbb{Q}}[\underline{X}]/\langle \tilde{f}_1, \dots, \tilde{f}_k \rangle) = n - k$ .*

*Proof.* We proceed by induction on  $k$ . The base of the induction is clear. Assume that we have found  $\tilde{f}_1, \dots, \tilde{f}_k$  with the desired properties and  $k < n - d$ . Now by Krull's height theorem and the fact that ring of polynomials is a catenary ring we have that  $\text{ht}(\mathfrak{a}) = k$  where  $\mathfrak{a} = \langle \tilde{f}_1, \dots, \tilde{f}_k \rangle$ . So by the unmixedness theorem we have  $\text{ht}(\mathfrak{p}) = k$  for any  $\mathfrak{p} \in \text{Ass}(\mathfrak{a})$ . Since  $\text{ht}(\langle f_1, \dots, f_m \rangle) = n - d > k$ , for any  $\mathfrak{p} \in \text{Ass}(\mathfrak{a})$  there is an  $i$  such that  $f_i \notin \mathfrak{p}$ . This implies that for any  $m$  distinct integers  $n_1, \dots, n_m$  and any  $\mathfrak{p} \in \text{Ass}(\mathfrak{a})$  we have that

$$\left\{ \sum_{i=1}^m n_j^i f_i \mid j = 1, \dots, m \right\} \not\subseteq \mathfrak{p}.$$

Therefore

$$(63) \quad \left\{ \sum_{i=1}^m j^i f_i \mid j = 1, \dots, l \right\} \not\subseteq \bigcup_{\mathfrak{p} \in \text{Ass}(\mathfrak{a})} \mathfrak{p},$$

where  $l = |\text{Ass}(\mathfrak{a})|(m - 1) + 1$ .

By the generalized Bezout theorem and the induction hypothesis  $|\text{Ass}(\mathfrak{a})| \ll 1$  where the implied constant depends on  $n$  and the degree of  $f_i$ . It is also well-known that the set of zero-divisors of  $\overline{\mathbb{Q}}[\underline{X}]/\mathfrak{a}$  is equal to  $\bigcup_{\mathfrak{p} \in \text{Ass}(\mathfrak{a})} \mathfrak{p}/\mathfrak{a}$ . So for some  $j \ll 1$ ,  $\tilde{f}_{k+1} = \sum_{i=1}^m j^i f_i$  modulo  $\mathfrak{a}$  is not a zero-divisor. Hence by Krull's principal ideal theorem, the fact that ring of polynomials is catenary and the above discussion, we have that  $\tilde{f}_{k+1}$  has the desired properties.  $\square$

*Proof of Proposition 66.* Similar to Weil restriction of scalars, we can fix a  $\mathbb{Q}$ -basis  $\mathfrak{B} := \{\alpha_i\}$  of  $k$  and get a polynomial  $R_{\mathfrak{B}}(f)$  over  $\mathbb{Q}$  from a polynomial  $f$  over  $k$ :

$$R_{\mathfrak{B}}(f)(\underline{X}^{(1)}, \dots, \underline{X}^{(\dim_{\mathbb{Q}} k)}) := f\left(\sum_i \alpha_i \underline{X}^{(i)}\right).$$

Notice that  $\deg R_{\mathfrak{B}}(f) = \deg f$ , the number of variables of  $R_{\mathfrak{B}}(f)$  is the number of variables of  $f$  times  $\dim_{\mathbb{Q}} k$ , and  $h(f) = \Theta_{\mathfrak{B}}(h(R_{\mathfrak{B}}(f)))$ . So without loss of generality, we can assume that  $k = \mathbb{Q}$ .

By Lemma 67 and Lemma 68, it is enough to prove that if

$$V(\overline{\mathbb{Q}}) = \{\mathbf{x} \in \overline{\mathbb{Q}}^n \mid f_1(\mathbf{x}) = \dots = f_n(\mathbf{x}) = 0\}$$

is a finite non-empty set where  $V = \text{Spec}(\overline{\mathbb{Q}}[\underline{X}]/\langle f_1, \dots, f_n \rangle)$ , Then for any  $\mathbf{x} \in V(\overline{\mathbb{Q}})$  we have that  $h(\mathbf{x}) \ll \max_i h(f_i)$ , where the implied constant depends on  $n$  and  $\max_i \deg f_i$ . And this is an easy corollary of arithmetic Bézout theorem [BGS94, Theorem 5.5.1].  $\square$



## REFERENCES

- [BY91] C. Bernstein, A. Yger, *Effective Bezout identities in  $\mathbb{Q}[z_1, \dots, z_n]$* , Acta Math. **166** (1991) 69–120.
- [BG06] E. Bombieri, W. Gubler, *Heights in Diophantine geometry*, Cambridge University press, New York, 2006.
- [BGS94] J.-B. Bost, H. Gillet, C. Soulé, *Heights of projective varieties and positive Green forms*, JAMS **7**, no. 4, (1994) 903–1027.
- [BFLM11] J. Bourgain, A. Furman, E. Lindenstrauss, S. Moses, *Stationary measures and equidistribution for orbits of non-abelian semigroups on the torus*, JAMS **24**, no. 1, (2011) 231–280.
- [BG08-a] J. Bourgain, A. Gamburd, *Uniform expansion bounds for Cayley graphs of  $SL_2(\mathbb{F}_p)$* , Ann. of Math. **167** (2008) 625–642.
- [BG08-b] J. Bourgain, A. Gamburd, *Expansion and random walks in  $SL_d(\mathbb{Z}/p^n\mathbb{Z})$ :I*, JEMS **10** (2008) 987–1011.
- [BG09] J. Bourgain, A. Gamburd, *Expansion and random walks in  $SL_d(\mathbb{Z}/p^n\mathbb{Z})$ :II. With an appendix by J. Bourgain*, JEMS **11**, no. 5., (2009) 1057–1103.
- [BGS10] J. Bourgain, A. Gamburd, P. Sarnak, *Affine linear sieve, expanders, and sum-product*, Invent. math. **179**, no. 3., (2010) 559–644.
- [BV12] J. Bourgain, P. Varjú, *Expansion in  $SL_d(\mathbb{Z}/q\mathbb{Z})$ ,  $q$  arbitrary*, Invent. math. **188**, no 1, (2012) 151–173.
- [BISG] R. Boutonnet, A. Ioana, A. Salehi Golsefidy, *Local spectral gap*, preprint, available online <http://arxiv.org/pdf/1503.06473.pdf>.
- [BGT11] E. Breuillard, B. Green, T. Tao, *Approximate subgroups of linear groups*, GAFA **21** (2011) 774–819.
- [BO14] E. Breuillard, H. Oh (editors), *Thin groups and superstrong approximation*, MSRI Publ. **61**, Cambridge Univ. Press., Cambridge 2014.
- [BS91] M. Burger and P. Sarnak, *Ramanujan duals II*, Invent. math. **106**, no. 1, (1991) 1–11.
- [Clo03] L. Clozel, *Démonstration de la conjecture  $\tau$* , Invent. math. **151**, no. 2, (2003) 133–150.
- [CU04] L. Clozel, E. Ullmo, *Equidistribution des points de Hecke*, Contributions to Automorphic Forms, Geometry and Arithmetic, (2004) volume in honor of Shalika, Johns Hopkins University Press, editors: Hida, Ramakrishnan and Shaidi, 193–254.
- [CFW81] A. Connes, J. Feldman, B. Weiss, *An amenable equivalence relations is generated by a single transformation*, Ergodic Th. Dynam. Sys. **1** (1981) 431–450.
- [Din06] O. Dinai, *Poly-log diameter bounds for some families of finite groups*, Proc. AMS **134**, no 11, (2006) 3137–3142.
- [DDMS99] J. Dixon, M. Du Sautoy, A. Mann, D. Segal, *Analytic pro- $p$  groups*, Cambridge University Press, Cambridge, 1999.
- [EHK12] J. Ellenberg, C. Hall, E. Kowalski, *Expander graphs, gonality, and variation of Galois representations*, Duke Math J. **161**, no. 7, (2012) 1233–1275.
- [EMO05] A. Eskin, S. Mozes, H. Oh, *On uniform exponential growth for linear groups*, Invent. Math. **160**, no. 1, (2005) 1–30.
- [FHJ94] M. D. Fried, D. Haran, M. Jarden, *Effective counting of the points of definable sets over finite fields*, Israel J. of Math. **85** (1994) 103–133.
- [Fur11] A. Furman, *A survey of Measured Group Theory, Geometry, Rigidity, and Group Actions*, The University of Chicago Press, Chicago and London, 2011, 296–374.
- [Gab10] D. Gaboriau, *Orbit equivalence and measured group theory*, In Proceedings of the ICM (Hyderabad, India, 2010), Vol. III, Hindustan Book Agency, 2010, 1501–1527.
- [Gam02] A. Gamburd, *On the spectral gap for infinite index “congruence” subgroups of  $SL_2(\mathbb{Z})$* , Israel J. Math. **127** (2002) 157–200.
- [GS04] A. Gamburd, M. Shahshahani, *Uniform diameter bounds for some families of Cayley graphs*, IMRN **71** (2004) 3813–3824.
- [Gow08] W.T. Gowers, *Quasirandom Groups*, Combinatorics, Probability and Computing **17** (2008) 363–387.
- [Hel05] H. Helfgott, *Growth and generation in  $SL_2(\mathbb{Z}/p\mathbb{Z})$* , Ann. Math. **167** (2008) 601–623.
- [Hel11] H. Helfgott, *Growth in  $SL_3(\mathbb{Z}/p\mathbb{Z})$* , JEMS **13**, no. 3, (2011) 761–851.
- [HLW06] S. Hoory, N. Linial, A. Wigderson, *Expander graphs and their application*, Bull. AMS **43**, no. 4, (2006) 439–561.
- [How77] R. Howe, *Kirillov theory for compact  $p$ -adic groups*, Pacific Journal of Mathematics **73**, no. 2, (1977) 365–381.
- [Hum95] J. Humphreys, *Linear algebraic groups*, Springer-Verlag, New York, 1995.
- [Ioa14-a] A. Ioana, *Orbit equivalence and Borel reducibility rigidity for profinite actions with spectral gap*, to appear in JEMS. Available online: <http://arxiv.org/pdf/1309.3026v4.pdf>
- [Ioa14-b] A. Ioana, *Strong ergodicity, property (T), and orbit equivalence rigidity for translation actions*, to appear in J. Reine Angew. Math. Available online: <http://arxiv.org/pdf/1406.6628.pdf>
- [Kaz67] D. Kazhdan, *On the connection of the dual space of a group with the structure of its closed subgroups*, (Russian) Funkcional. Anal. i Priložen. **1** (1967) 71–74.
- [Kes59] H. Kesten, *Symmetric random walks on groups*, Trans. Amer. Math. Soc. **92** (1959) 336–354.
- [LS74] V. Landazuri, G. M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, Journal of Algebra **32** (1974) 418–443.
- [LW54] S. Lang, A. Weil, *Number of points of varieties in finite fields*, American Journal of Mathematics **76**, no. 4, (1954) 819–827.
- [Lub94] A. Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures*, Birkhäuser, 1994.

- [Lub95] A. Lubotzky, *Cayley graphs: eigenvalues, expanders and random walks*, In: Rowbinson, P. (ed.) *Surveys in Combinatorics*. London Math. Soc. Lecture Note Ser. **218** 155–189, Cambridge University Press, Cambridge, 1995.
- [LM13] A. Lubotzky, C. Meiri, *Sieve methods in group theory I: powers in linear groups*, JAMS **25**, no. 4, (2012) 1119–1148.
- [Mar73] G. Margulis, *Explicit constructions of expanders*, Problemy Peredaci Informacii **9**, no. 4, (1973) 71–80.
- [MW83] D.W. Masser, G. Wüstholz, *Fields of large transcendence degree generated by values of elliptic functions*, Invent. Math. **72**, no. 3, (1983) 407–464.
- [NP11] N. Nikolov, L. Pyber, *Product decompositions of quasirandom groups and a Jordan type theorem*, JEMS **13**, no. 4, (2011) 1063–1077.
- [Nor89] M. V. Nori, *On subgroups of  $GL_n(\mathbb{F}_p)$* , Invent. Math. **88**, no. 2, (1987) 257–275.
- [OW80] D. Ornstein, B. Weiss, *Ergodic theory of amenable groups. I. The Rokhlin lemma.*, Bull. AMS (N.S.) **1** (1980) 161–164.
- [Pop07] S. Popa, *Deformation and rigidity for group actions and von Neumann algebras*, In Proceedings of the ICM (Madrid, 2006), Vol. I, European Mathematical Society Publishing House, 2007, 445–477.
- [PS] L. Pyber, E. Szabó, *Growth in finite simple groups of Lie type*, JAMS, accepted. Available online: <http://arxiv.org/abs/1005.1858>
- [SG05] A. Salehi Golsefidy, *Character degrees of  $p$ -groups and pro- $p$  groups*, Journal of Algebra **286** (2005) 476–491.
- [SG-a] A. Salehi Golsefidy, *Super-approximation, II: the  $p$ -adic and bounded power of square-free integers cases.*, preprint.
- [SG-b] A. Salehi Golsefidy, *Sum-Product phenomenon: the local field case*, preprint.
- [SGV12] A. Salehi Golsefidy, P. Varjú, *Expansions in perfect groups*, GAFA **22**, no. 6, (2012) 1832–1891.
- [SGS13] A. Salehi Golsefidy, P. Sarnak, *Affine sieve*, JAMS **26**, no. 4, (2013) 1085–1105.
- [SX91] P. Sarnak and X. Xue, *Bounds for multiplicities of automorphic representations*, Duke Math. J. **64**, no. 1, (1991) 207–227.
- [Sel65] A. Selberg, *On the estimation of Fourier coefficients of modular forms*, Proc. Sympos. Pure Math., Vol. VIII, AMS, Providence, RI, 1965, 1–15.
- [Sha09] A. Shalev, *Word maps, conjugacy classes, and a noncommutative Waring-type theorem*, Ann. of Math. (2) **170**, no. 3, (2009) 1383–1416.
- [Ste65] R. Steinberg, *Regular elements of semisimple algebraic groups*, Publication of IHES **25** (1965) 49–80.
- [Tao08] T. Tao, *Product set estimates for non-commutative groups*, Combinatorica **28**, no. 5, (2008) 547–594.
- [Var12] P. Varjú, *Expansion in  $SL_d(\mathcal{O}_K/I)$ ,  $I$  square-free*, JEMS **14**, no. 1, (2012) 273–305.
- [Wei84] B. Weisfeiler, *Strong approximation for Zariski-dense subgroups of semisimple algebraic groups*, Ann. Math. **120** (1984) 271–315.

MATHEMATICS DEPT, UNIVERSITY OF CALIFORNIA, SAN DIEGO, CA 92093-0112

*E-mail address:* golsefidy@ucsd.edu